تُعد الرخصة الأوربية لقيادة الحاسب الآلي (ECDL) والرخصة الدولية لقيادة الحاسب الآلي (ICDL) وبرنامج المواطن الإلكتروني وجميع الشعارات ذات الصلة من العلامات التجارية المسجلة لمؤسسة الرخصة الأوربية لقيادة الحاسب الآلي المحدودة (ICDL).

وقد تُستخدم هذه البرامج التعليمية لمساعدة المرشحين في التحضير لبرنامج شهادة مؤسسة الرخصة الأوربية لقيادة الحاسب الآلي، وتجدر الإشارة إلى أن مؤسسة الرخصة الدولية لقيادة الحاسب الآلي لا تتعهد بتقديم أي ضمانات تفيد بأن استخدام البرامج التعليمية يضمن اجتياز برنامج شهادة المؤسسة.

لا تضمن المواد الواردة في هذه الدورة الدراسية أن المرشحين سيجتازون اختبار برنامج شهادة مؤسسة الرخصة الدولية لقيادة الحاسب الآلي، كما أن كافة مواد التقييم أو تمارين الأداء الموجودة في هذا البرنامج تتعلق فقط بهذا المنشور، وأنها لا تشكّل شهادة من مؤسسة الرخصة الدولية لقيادة الحاسب الآلي أو تحملها، وذلك فيما يتعلق ببرنامج شهادة مؤسسة الرخصة الأوروبية لقيادة الحاسب الآلي أو أي اختبار آخر لمؤسسة الرخصة الدولية لقيادة الحاسب الآلي، هذا ولا تمثل هذه المواد أي شهادة، ولا تؤدي إلى الحصول عليها من خلال أي ممارسات أخرى دون اختبار شهادة مؤسسة الرخصة الدولية لقيادة الحاسب الآلي.

يتعين على المرشحين ممن يستخدمون مواد البرامج التعليمية التسجيل في برامج المشغّل الوطني قبل إجراء اختبار برنامج شهادة مؤسسة الرخصة الدولية لقيادة الحاسب الآلي، فبدون هذا التسجيل لن يتمكن المرشح من الخضوع للاختبارات أو الحصول على شهاداتها أو على أي وجه من أوجه الاعتراف بها، على أن يكون التسجيل في مركز اختبار معتمَد.

الرخصة الدولية لقيادة الحاسب الآلي – الامن السيبراني للمعلمين

شهادة الرخصة الدولية لقيادة الحاسب الآلي

الأمن السيبراني للمعلمين في بيئة التعليم من مرحلة رياض الاطفال و حتى الثاني عشر.

تم تطوير هذا البرنامج التعليمي لتزويد المعلمين والمدرسين ومسؤولي المؤسسات الأكاديمية بنظرة شاملة عن الأمن السيبراني للمجال التعليمي. سيوفر محتواها فهمًا للمخاطر التي يمكن ان يواجهها الطلاب الذين يعملون عبر الإنترنت وكيف يمكن للمعلمين تحديد هذه المخاطر والرد عليها.

يستهدف محتوى الكتاب المعلمين والمعلمات وليس الأطفال ، وبالتالي تم تضمين مواضيع المواد الإباحية والرسائل الجنسية والموضوعات الحساسة الأخرى ذات الصلة. تم تناول هذه الموضوعات بحساسية ثقافية للمنطقة العربية. هدفنا هو التأكد من أن التربويين و القائمين على تربية الأطفال يدركون تمامًا جميع المخاطر ويمكنهم اتخاذ قرارات مستنيرة بشأن جميع الموضوعات المتعلقة بالسلامة الإلكترونية. نأمل ألا يكون هناك أي جريمة بإدراج هذه الموضوعات الهامة حيث انها تكون بغير قصد.

أهداف المقرر

بعد اجتياز هذا المقرر سيتمكن المرشحون من :

1. التعرف على المخاطر الأمنية المحتملة على الطلاب المشاركين في مختلف الأنشطة عبر الإنترنت.
2. تطوير وتحديث وعي المعلمين وفهمهم لحماية الطلاب للمساعدة في الحفاظ على أمان الطلاب عبر الإنترنت.
3. فهم كيفية إنشاء خطط فعالة للمساعدة في حماية الطلاب عبر الإنترنت ، بما في ذلك دعم اهتمامات أولياء الأمور.
4. استخدم الأدوات والتقنيات المختلفة لتأمين وحماية الطلاب من خلال تجاربهم على الإنترنت.
5. التعرف على الطرق العملية للحفاظ على أمان الطلاب ، مثل محركات البحث الصديقة للطفل ، وإعدادات الخصوصية ، وبرامج الرقابة الأبوية.
6. تطوير الوعي بالمخاطر على الإنترنت ، مثل التسلط عبر الإنترنت ، والرسائل غير المناسبة ، والتحرش الجنسي ، ومواقع الويب غير الملائمة ، والتطرف على الإنترنت ، والمشاركة (البث) عبر الإنترنت والاستخدام غير المناسب لمواقع الشبكات الاجتماعية.
7. التعرف على كيفية مساعدة الطلاب على إدارة المخاطر الامنية على الإنترنت ، بما في ذلك التحدث مع الطلاب حول المحتوى والأنشطة عبر الإنترنت.
8. فهم التشريعات ذات الصلة والتوجيهات الأخلاقية لحماية الطلاب.
9. التعرف على الأنواع المختلفة للمخاطر الامنية وعلامات البلطجة عبر الإنترنت ، لتوفير استجابة مناسبة للطلاب المشاركين.
10. التعرف على العناصر الرئيسية لسياسات وإجراءات الأمن السيبراني.
11. تتبع التغييرات في سلوك الأطفال على الإنترنت ، وتوعيتهم بالتطورات والمخاطر الجديدة.
12. فهم مجموعة من مبادرات الامان، مثل الوعي والاستراتيجيات والقواعد التي تنظم عملية الوصول للأنترنيت و استخداماتها. وكذلك أيضًا بناء مرونة رقمية لدى الأطفال من خلال السلامة والخصوصية.
13. فهم كيفية استخدام سياسات الأمان والموارد المتاحة.

14. فهم وتطبيق مفاهيم ومبادئ التفكير الأخلاقي على المشاكل المتعلقة بأجهزة الكمبيوتر والتقنيات الرقمية.

15. تعريف القضايا القانونية ومعرفة ما سيحدث عندما ينتهك الطالب قوانين الإنترنت.

تستند هذه الوحدة إلى الممارسات والتجارب الدولية للأمن السيبراني للمعلمين ، وخصوصًا معلمي المراحل من رياض الاطفال وحتى الصف الثاني عشر (K-12) من العديد من الدول الرائدة في مجال التعليم ، بما في ذلك:

1. The UK Council for Child Internet Safety (UKCCIS)- Government of UK
2. UK Safer Internet Centre
3. Research Paper: children's use of the internet – London School of Economics and Political Science (LES)
4. Organization Stop it Now- UK and Ireland
5. Australian Parenting Website
6. Office of the E-safety Commissioner- Government of Australia
7. Federal Trade Commission – Protecting American's Consumer – US
8. The Privacy Technical Assistance Centre - U.S. Department of Education
9. COSN Leading Education Innovation- Norway and Finland Built *Innovative*, Trusted *Educational* Environments.
10. The K-12 Cybersecurity Resource Centre-Department of Education – Ohio - US
11. Canada's Centre for Digital and Media Literacy
12. National Crime Agency – Child Line – UK
13. US News Education
14. The Security Awareness Company (SAC) –US
15. Office of Education Technology (OET)
16. Security Best Practices Guideline for Districts- Kentucky Department of Education
17. City University of New York (CUNY) CUNY Academic Works- US
18. United Nations Educational, Scientific and Cultural Organization
19. Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University
20. Council of the Great City School – Baltimore City Public School – USA
21. National Cybersecurity Centre- Government of UK

جدول المحتويات

القسم 1: استخدام شبكات الإنترنت والتواصل الاجتماعي في المدارس

1-1 استخدام الإنترنت

1-1- 1 الفوائد التي تعود على الطالب من استخدام شبكة الإنترنت

يُعد الانترنت من الأدوات المفيدة جدًا لطلاب المدارس في نواحي كثيرة، حيث يتمكن الطالب من استرجاع معلومات ذات صلة بدراسته بالاستعانة بالعديد من المواقع الإلكترونية، كما يمكن أن يكون بمثابة مُعلم، ويمكن للطلاب استخدام الإنترنت للبحث عن أي شيء وللتواصل مع المعلمين والطلاب الآخرين وللقيام بالواجب المنزلي ولتقديم المساعدة، ويمكن لهم أيضًا تلقي الدروس والاختبارات عبر الإنترنت ومشاهدة مقاطع الفيديو ذات الصلة، إذ كان الإنترنت سببًا في ثورة العالم من التعليم إلى العمل.

1- مواد الدراسة ذات الصلة: يوفر الإنترنت معلومات لا نهائية، ويمكن للطلاب دراسة المواد ذات الصلة من خلال العديد من المواقع المختلفة المتعلقة بموضوع الدراسة.

التعليم الإلكتروني: يسهم التعليم الإلكتروني في جعل التعلم أكثر سهولة.

التواصل الموثوق: لا يوفر الإنترنت التعليم فقط، ولكن يمكن استخدامه كطريقة للتواصل بين الطالب والمعلم، بحيث يتمكن الطلاب من مشاركة أفكارهم بشأن موضوع ما ويرد المعلم عليهم مباشرة، بحيث يتم التواصل بشأن أداء الطلاب وتقديم معلومات واضحة عن المشاريع وغير ذلك من المراسلات بصورة سريعة.

استرجاع المعلومات:

- ✓ تعد زيادة إمكانية الوصول إلى المواد المرجعية والبيانات من أهم مزايا الإنترنت في مجال البحث عن المعلومات وهو متاح لجميع فئات المستخدمين.
- ✓ من المنظور العالمي، توجد إمكانية لتقليص الفجوة المتعلقة بنوع وكم المعلومات المقدمة للتعلم في البلدان المتقدمة والبلدان النامية.
- ✓ يُمثل انخفاض تكلفة تقديم المعلومات للمستخدمين أحد الإنجازات الأخرى لتقنيات الشبكات العالمية.

2- **التعليم والتعلم الفردي:** لا يمكن التقليل من أهمية وسائل التواصل من نوع "شخص إلى شخص" على الإنترنت، **حيث يمتلك الإنترنت ميزة إنشاء الشبكات، لذا يعتبر معظم الباحثين الإنترنت وسيلة اتصال جماهيري.**

3- **الأنشطة التعاونية:** يتم تحديد المزايا التي توفرها شبكة الإنترنت في تنظيم التعاون مسبقًا حسب طبيعة الشبكة، وهي تُعرف بشبكة الويب العالمية وتم تأسيسها كبيئة للعمل الجماعي بوثائق مشتركة مقدمة من باحثين يعيشون في مناطق بعيدة عن بعضهم البعض. ويوفر المزيد من التطوير لتكنولوجيا الإنترنت فرصًا للاستخدام التعاوني وتحرير المواد النصية والجداول الزمنية وتسلسل الأصوات والفيديو.

- ✓ يُظهر المعلمون إمكانيات استخدام الإنترنت في سيناريوهات تعليمية مختلفة.
- ✓ يقدم المعلمون فرصًا لتفضيل عملية التدريب الدائمة والإرشادات المقدمة من قبلهم من خلال استغلال إمكانات الإنترنت في مهامهم التعليمية.



2-1-1 لماذا تُعد إجراءات أمان الانترنت من الأمور المهمة؟

يدخل الطلاب الذين هم في سن المدرسة إلى شبكة الإنترنت لمشاهدة مقاطع الفيديو وممارسة الألعاب والتواصل مع الأصدقاء وأفراد العائلة، كما أنهم يستخدمون الإنترنت في الأعمال المدرسية والواجبات المنزلية، ويستخدم الطلاب شبكة الانترنت من خلال أجهزة الكمبيوتر والهواتف المحمولة والأجهزة اللوحية وأجهزة التلفاز والأجهزة الأخرى. وقد بدأ وصول الطلاب الذين هم في سن المدرسة إلى مواقع الإنترنت منفردين ودون إشراف في بعض الحالات، لذلك هناك مخاطر تتعلق بأمان الإنترنت أكثر من أي وقت مضى، فهناك مخاطر محددة في حالة استخدام الطلاب الإنترنت للتواصل مع الآخرين - على سبيل المثال، استخدام وسائل التواصل الاجتماعي أو اللعب عبر الإنترنت، وعند التحدث عن بعض احتياطات الأمان العملية، يمكن للمدرسين حماية الطلاب من المحتوى والأنشطة الخطرة أو غير المناسبة من خلال اتخاذ بعض الاحتياطات العملية لأمان الإنترنت، ويستمر الطلاب في الاستفادة إلى أقصى درجة ممكنه من التجارب عبر الإنترنت، وإمكانية التعلم والاستكشاف والإبداع والتواصل مع الغير، فغالبًا ما يملك الطلاب أجهزتهم الخاصة التي يستخدمونها للاتصال بالإنترنت، فهم يستخدمون الوسائط الرقمية والإنترنت للقيام بالأعمال المدرسية والواجبات المنزلية واللعب وتنزيل مقاطع الموسيقى أو الاستماع إليها والتصفح العام، ويمكنهم أيضًا التواصل مع أشخاص آخرين من خلال تطبيقات الدردشة داخل الألعاب ووسائل التواصل الاجتماعي الأخرى. ومع تزايد دخول الطلاب إلى الإنترنت بصورة منفردة ازدادت المخاطر المتعلقة بالأمان.

2-1 استخدام وسائل التواصل الاجتماعي

1-2-1 الفوائد التعليمية المرتبطة باستخدام الهواتف المحمولة ووسائل التواصل الاجتماعي

يكتسب الطلاب والمدارس فوائد تعليمية هامة من استخدام الهواتف المحمولة ووسائل التواصل الاجتماعي، وهناك اعتراف متزايد من جانب المعلمين وخبراء الدعم التعليمي ومدراء المدارس وخبراء التعليم البارزين بأن التقنيات الرقمية الجديدة أُنشئت لتبقى، كما أنها تقدم فوائد تعليمية كبيرة إذا تم استخدامها بصورة صحيحة. وبالرغم من وجود فوائد كثيرة إلا أنها لا تخلو من المخاطر. ويتعين على واضعي السياسات والمربين مراعاة العواقب قبل اتخاذ خطوات لفرض قيود على استخدام وسائل التواصل الاجتماعي وتقنيات الهواتف المحمولة في المدارس. ويشير بهذا النموذج إلى أهمية دراسة مثل هذا الإجراء بعناية ومراعاة مزايا وسائل التواصل الاجتماعي للتعلم، فالإرشادات ضرورية للاستخدام المسؤول حتى يتمكن الطلاب من استكشاف المعلومات ومشاركتها بأمان. ويُعد السماح باستخدام وسائل التواصل الاجتماعي في الفصل من أهم طرق تعريف الطلاب بكيفية استخدام أجهزتهم بأمان، ويجب استخدام التكنولوجيا في مكان خاضع لإشراف يؤكد تطوير الاتجاهات والمهارات، بما يساعد الطلاب في الحفاظ على سلامتهم داخل المدارس وخارجها. ويعد تدريب خلف عجلة القيادة من الدراسات المستخدمة في هذا المجال وهو لا يقل أهمية عن الدراسات النظرية لـ "قواعد الطريق". ولمواصلة التفكير في القضايا المعنية، تقدم الأقسام التالية ملخصًا للمواضيع المُستجدة المتعلقة بالاستخدامات التعليمية من خلال وسائل التواصل الاجتماعي وتختتم بتوصيات بشأن السياسات المسؤولة.

2-2-1 وسائل التواصل الاجتماعي للطلاب

وسائل التواصل الاجتماعي: هو مصطلح يطلق على المنصات الإلكترونية التي يستخدمها الأشخاص للتواصل مع الآخرين و مشاركة محتوى الوسائط المتعددة وتكوين الشبكات الاجتماعية. وتعتبر الألعاب متعددة اللاعبين مثل **Minecraft**، **World of Warcraft** و **League of Legends** و **Fortnite** و **The Sims** من المنصات الأكثر شعبية على الإنترنت، حيث يتصل الطلاب باللاعبين الاخرين ويتحدثون معهم أثناء اللعب.

و تعتبر مواقع العاب الدردشة طرقًا شائعة للطلاب للتواصل مع الآخرين الذين يشاركونهم الاهتمام في ألعاب مماثلة.

تُعد وسائل التواصل الاجتماعي منصة إلكترونية يستخدمها الأشخاص للتواصل مع الآخرين ومشاركة محتوى الوسائط وتكوين شبكات اجتماعية، وتعتبر الألعاب التي يشارك فيه أكثر من لاعب من أكثر المنصات شيوعًا على الإنترنت، بما في ذلك وورلد أوف ووركرافت وليج أوف ليجيندز وفورتنايت وذا سيمز، حيث يتواصل الطلاب بلاعبين آخرين ويتحدثون إليهم أثناء اللعب، وتعد مواقع دردشة الألعاب من الطرق المحببة لدى الطلاب أيضًا لتواصل مع أشخاص آخرين لديهم نفس اهتمامات اللعب.

استخدام وسائل التواصل الاجتماعي من خلال تحميل ومشاركة المحتوى. ويشمل ذلك ما يلي:

- ✓ إنشاء ملفات تعريف عبر الإنترنت
- ✓ نشر التعليقات أو الدردشة
- ✓ تحميل الصور ومقاطع الفيديو
- ✓ مشاركة الروابط

- ✓ وضع علامات على الصور والمحتوى
- ✓ إنشاء ومشاركة تعديلات اللعبة
- ✓ إعادة تعديل المحتوى الموجود أو تغييره ومشاركته

1-2-3 ما هي الفوائد التي تعود على الطلاب من استخدام وسائل التواصل الاجتماعي؟

تشكل وسائل التواصل الاجتماعي جانبًا حيويًا من حياة الطلاب الاجتماعية والإبداعية، فهم يستخدمون وسائل التواصل الاجتماعي لقضاء أوقات ممتعة وتكوين صداقات ومشاركة الاهتمامات واستكشاف الهويات وإقامة علاقات مع أفراد العائلة، فذلك هو امتداد لتواصلهم في الواقع الفعلي. وتمكن وسائل التواصل الاجتماعي من اتصال الطلاب بالمجتمعات العالمية بناءً على اهتمامات مشتركة، وقد يتمثل ذلك في شبكات الدعم - على سبيل المثال، الطلاب ذوو الإعاقة أو من لديهم حالة مرضية خاصة أو من نفس الجنس أو من لديهم خلفية ثقافية محددة، كما قد تكون هناك مواقع للتعليق ومشاركة المحتوى بشأن اهتمامات محددة مثل الرياضة أو الألعاب أو المسلسلات التلفزيونية أو الموسيقى أو الهوايات.

ويكتسب الطلاب العديد من الفوائد الأخرى عند استخدام وسائل التواصل الاجتماعي، وتشمل:

- ✓ **الاستكشاف والتجربة**: تساعد وسائل التواصل الاجتماعي الطلاب في بناء المعارف والمهارات اللازمة للاستمتاع بالأنشطة عبر الإنترنت وتجنب المخاطر المتعلقة بها.
- ✓ **التعلم التشاركي:** يتمكن الطلاب من استخدام وسائل التواصل الاجتماعي لمشاركة محتوى تعليمي سواء أكان ذلك في إطار دراسة رسمية أو غير رسمية.
- ✓ **الإبداع:** يمكن أن يكون الطلاب مبدعين فيما يخص إنشاء الملف الشخصي الخاص بهم وكذا الصور والفيديوهات وإدخال بعض التعديلات على الألعاب.
- ✓ **الصحة العقلية والرفاهية:** يوفر التواصل مع العائلة الكبيرة والأصدقاء والمشاركة في المجتمعات المحلية والعالمية شعورًا بالانتماء.

1-2-4 نظرة عامة على استخدام وسائل التواصل الاجتماعي الشائعة

1- **فيسبوك**: يعد فيسبوك من الوسائط الاجتماعية التي تسمح للمستخدمين بإنشاء ملف تعريف على الإنترنت مع إضافة تفاصيل شخصية وصور ومقاطع فيديو وغير ذلك من المعلومات، كما يتمكن المستخدمون من إضافة أصدقاء وإرسال رسائل وإخبار الأصدقاء بما يقومون به من خلال تحديثات الحالة، كما يتمكن المستخدمون أيضًا من التعليق على تحديثات الأصدقاء وصورهم ومقاطع الفيديو الخاصة بهم.

2- **تويتر:** يعد تويتر من الوسائط الاجتماعية التي تسمح بإرسال واستقبال رسائل قصيرة جدًا يطلق عليها تغريدات، ويمكن أن تشتمل التغريدات على روابط تشعبية أو صور. ولاستلام رسائل على الجدول الزمني لتويتر، يجب عليك متابعة الأشخاص الذين تهتم بهم لتلقي الرسائل وكي يتبعك أشخاص آخرون.

3- **واتساب:** يُستخدم هذا التطبيق الاتصال عبر الإنترنت في الهواتف المحمولة لإرسال واستقبال الرسائل والمكالمات والصور ومقاطع الفيديو والرسائل الصوتية.

4- **تمبلر:** يعد تمبلر أحد مواقع التواصل الاجتماعي والمدونات الصغيرة (أحد أشكال المدونات القصيرة)، حيث يتمكن المستخدمون من نشر ومشاركة النصوص والصور والاقتباسات والروابط والموسيقى ومقاطع الفيديو من متصفحات الويب أو الهواتف أو سطح المكتب أو البريد الإلكتروني إلى صفحة المدونة الخاصة بهم.

5- **إنستجرام:** إنستجرام هو تطبيق مشاركة الصور عبر الإنترنت وشبكات التواصل الاجتماعي التي تسمح للمستخدمين بتحرير الصور ومقاطع الفيديو القصيرة وتحميلها من خلال تطبيقات محمولة. ويمتلك المستخدمون الخيار في جعل ملفاتهم الشخصية خاصة، وفي هذه الحالة سيتمكن متابعيهم فقط من رؤية منشوراتهم.

6- **سكايب:** تمكن خدمة سكايب المستخدمين من إجراء دردشة عبر الإنترنت وإجراء مكالمات صوتية ومرئية مع مستخدمين آخرين والاتصال بأرقام هواتف أرضية أو محمولة.



7- **يوتيوب:** يمكن موقع يوتيوب من تحميل مقاطع الفيديو وعرضها ومشاركتها. وتشمل مقاطع الفيديو على يوتيوب مقاطع من برامج تلفزيونية وأفلام إضافةً إلى مقاطع فيديو تم تصويرها في المنزل ومدونات الفيديو.

8- **فايبر:** يستخدم هذا التطبيق الاتصال بشبكة الإنترنت في الهواتف المحمولة للسماح للمستخدمين بإرسال رسائل نصية ومشاركة الصور ومقاطع الفيديو وإجراء مكالمات صوتية ومكالمات الفيديو.

9- **سناب شات:** يمكن هذا التطبيق من مشاركة الصور ومقاطع الفيديو وكذلك الدردشة عن طريق كتابة النصوص أو الصوت أو الفيديو عبر شبكة WiFI، كما يتمكن المستخدمون من التقاط الصور وتسجيل مقاطع الفيديو والنصوص والرسومات وإرسالها إلى قائمة محددة من المشاهدين. ويحدد المستخدمون مهلة زمنية لمشاهدة صورهم، إلا إنه يسمح للمشاهدين بأخذ لقطات للشاشة والاحتفاظ بالصور.

10- **ماي سبيس:** موقع ماي سبيس هو شبكة تواصل اجتماعي كلاسيكية، حيث يتمكن المستخدمون من تبادل الرسائل والأفكار، وغالباً ما يستخدمه الموسيقيون لتقديم أعمالهم الخاصة.

11- **ميكسي:** تُعد شبكة ميكسي إحدى أكثر الشبكات الاجتماعية استخدامًا في اليابان، فهي تضم ما يقارب 20 مليون مستخدم مشارك في التفاعلات المجتمعية، حيث يتمكن المستخدمون من إرسال الرسائل واستقبالها وتقديم أنفسهم على صفحات ملفاتهم الشخصية والتفاعل مع أشخاص آخرين في المجتمع المحلي.

12- **أوركوت:** يُعد أوركوت شبكة اجتماعية عالمية تديرها جوجل، وهي مشهورة جدًا في البرازيل والهند، ولكنها تتشابه مع العديد من منصات التواصل الاجتماعي الأخرى،

إذ أنها تسمح للمستخدمين بالتعرف على أصدقاء جدد والاحتفاظ بالمعارف الحالية من خلال نشر رسائل تحديث الحالة وصور شخصية.

القسم 2: أنشطة الإنترنت

2-1 مخاطر إيذاء الطلاب عبر شبكة الإنترنت

2-1-1 إدراك المخاطر والأضرار

الخطر هو احتمال حدوث موقف عند التعرض لأمر خطير أو ضار، وتزداد احتمالية تعرض الشخص لمخاطر مع كثرة دخوله إلى شبكة الإنترنت، حيث يتصفح المستخدمون الإنترنت للحصول على محتوى ما عن طريق الأجهزة المحمولة، كأجهزة الكمبيوتر المحمول والهواتف المحمولة وأنظمة الألعاب ومشغلات الوسائط المحمولة. ومن المُرجح أن يواجه الطلاب الذين يستخدمون الإنترنت بكثرة بعض المخاطر والأضرار، ولكن لا تقتصر مهمة السياسة في منع المخاطر جميعها، بل في إدارة المخاطر بحيث يكون الطلاب مستعدين لها وقادرين على التعلم من المخاطر الأقل حدة، بينما يتم استخدام الموارد لتقليل الضرر وخاصة في حالات المخاطر الشديدة، ولا تؤدي المخاطر حتماً إلى وقوع ضرر، بل تثير قلقًا من احتمالية حدوث ضرر للطالب.



2-1-2 ما هي الأشياء التي يعتبرها الطلاب أمورًا مزعجة

يجب أن يكون المعلمين على دراية بالأمور التي تزعج الطلاب عند اتصالهم بالإنترنت، إذ تشكل المواد الإباحية والعنف جزءًا كبيرًا من مخاوف الطلاب، فيمكن القول أن أغلبهم قد شاهد مثل تلك المحتويات المزعجة على مواقع مشاركة الفيديوهات مثل يوتيوب أو شبكات التواصل الاجتماعي، وربما تواصلوا مع أشخاص غرباء أرادو أن يكون أصدقاءً لهم أو رأوا محتويات جنسية عبر الإنترنت جعلتهم يشعرون بعدم الارتياح، ويوجد "الكثير والكثير" من الإعلانات عبر الإنترنت بما في ذلك النميمة والشائعات. ومن جهة أخرى، قد يشعر الطلاب بالقلق حيال بصماتهم الرقمية التي قد تتسبب في وقوع مشكلات لهم لاحقًا إلى جانب سرقة الهوية الرقمية، كما توجد العديد من المخاطر المتعلقة باستخدام المعلومات

الرقمية، إذ تختلف المعلومات الرقمية اختلافًا كبيرًا عن نظيرتها المادية، حيث تتصف المعلومات المادية بثابت مواضعها عبر المكان والزمان. وهذا ليس شأن المعلومات الرقمية والتي يمكن أن تكون:

1- **سريعة التكرار وسهلة التوزيع:** حيث يتم إعادة إرسال الرسائل المنشورة عبر وسائل التواصل الاجتماعي في أماكن أخرى من قبل الأصدقاء أو رسالة بريد إلكتروني يتم إرسالها إلى قائمة من المستلمين خلال فترة زمنية قصيرة جدًا.

2- **مُخزنة في مواقع متعددة:** يمكن تخزين الصور على جهاز كمبيوتر محمول وهاتف ذكي وفي السحابة في الوقت ذاته.

3- **إمكانية الإنشاء والتوصيل التلقائي**: يمكن للهاتف الذكي مزامنة رسائل البريد الإلكتروني مع جهاز آخر أو مع خدمات متاحة عبر الإنترنت.

4- **مُخزنة بمستويات مختلفة من "إمكانية الاكتشاف":** لا يمكن الوصول إلى ملفات الصور إلا باستخدام كلمة مرور أو طريقة مصادقة أخرى.

5- **يمكن إيصال المعلومات الرقمية بسرعة:** تمكن الطبيعة "الفيروسية" للاتصالات الرقمية من نشر المعلومات بسرعة والوصول إلى جمهور عريض، وقد يصعب ذلك من التعرف على مَن تلقى المعلومات أو كيف سيتم نشرها فيما بعد، كما يتطلب ذلك أيضًا اتخاذ إجراء سريع لتقليل الضرر الذي قد ينجم عن هذا الاتصال إلى الحد الأدنى.

6- **صعوبة حذف المعلومات الرقمية بصورة نهائية:** بمجرد إنشاء محتوى رقمي يكون من الصعب، إن لم يكن من المستحيل، حذف النسخ جميعها نهائيًا. فعلى سبيل المثال يمكن أن تكون المعلومات الرقمية:

- ✓ مخزنة على مجموعة من الأجهزة الرقمية مثل الهواتف الذكية وأجهزة الكمبيوتر المحمولة وخوادم الإنترنت عند إرسالها، بما في ذلك رسائل البريد الإلكتروني أو رسائل الدردشة.
- ✓ يتم نسخها وإيصالها تلقائيًا أو حسب جدول زمني مما يجعل من الصعب معرفة المعلومات التي تم تخزينها وأين تم ذلك، فعلى سبيل المثال، يقوم الهاتف الذكي بمزامنة المعلومات المخزنة تلقائيًا مع كمبيوتر محمول أو "سحابة".
- ✓ تم الاسترجاع أو الاستعادة من الأرشيف أو سلة المحذوفات بعد الحذف باستخدام أدوات يمكن الوصول إليها بسهولة.
- ✓ تُخزن لفترة مؤقتة على الجهاز، فعلى سبيل المثال، سيقوم الجهاز بتنزيل المعلومات لعرض موقع ويب ثم حذفه عند إغلاق متصفح الويب.

7- **يمكن الوصول إلى المعلومات الرقمية عن بُعد:** وكذلك يمكن الوصول عن بُعد إلى أجهزة الإرسال الرقمية مثل الهواتف الذكية أو أجهزة الكمبيوتر المحمول من خلال اتصال إنترنت آخر، كما يمكن الوصول إلى محتوى موقع إلكتروني وتحريره عن بُعد، وتشمل أمثلة الإجراءات التي يمكن تنفيذها عن بعد ما يلي:

- ✓ حذف أو إضافة المعلومات المخزنة على جهاز رقمي أو صفحة ويب أو تحريرها.
- ✓ الوصول إلى خدمات موقع الجهاز للعثور على موقعه المحدد أو تشغيل كاميرا الويب الخاصة بالجهاز واستخدامه للتسجيل.

2-2 مخاطر سلامة الإنترنت على الطلاب

2-2-1 نظرة عامة على مخاطر الإنترنت

قد تكون المعلومات الخاطئة التي قد تظهر على مواقع شبكات التواصل الاجتماعي مقصودة أو غير مقصودة، بما في ذلك الشائعات المنشورة من قبل مستخدمين آخرين، ومن الأمثلة النموذجية لمخاطر المحتوى الاستفزازي التي قد يطلع عليه الطلاب رسائل الكراهية، فعندما ينشر شخص ما دعاية ما يمكن إساءة فهمها على أنها معلومات حقيقية، يتحول الأمر إلى مشكلة، وتشمل الفئة الثانية من المخاطر على مخاطر الاتصال. وبخلاف الرسائل الفورية، تعد مواقع شبكات التواصل الاجتماعي من أشهر الوسائط المستخدمة للتنمر على الإنترنت، وتُستخدم أيضًا للإغواء الجنسي عندما يرسل شخص ما رسائل جنسية، كما تزيد إمكانية الحصول على معلومات الاتصال عن طريق تصفح مواقع الرسائل الفورية من مخاطر الاتصال في أوقات عدم الاتصال بالإنترنت، إضافةً إلى ذلك، يواجه الطلاب على وجه الخصوص مخاطر تتعلق بالخصوصية، نظرًا لأنهم ينشرون الكثير من المعلومات الشخصية والتي قد تؤدي إلى التسلط في بعض الأحيان عبر الإنترنت، كما يحتفظ المراهقون بملف شخصي عام ولا يعرفون شيئًا عن إعدادات الخصوصية، بحيث يتمكن أصدقاء الأصدقاء من رؤية صفحاتهم، وقد يبدو أصدقاء الأصدقاء أشخاص عاديون، إلا أن معظمهم أشخاص غرباء لا نعرفهم على الإطلاق، وتشمل مخاطر الفئة الثالثة على المخاطر التجارية، وهذا يشمل إساءة استخدام البيانات الشخصية، إذ يمكن مشاركة المعلومات مع طرف ثالث من خلال التطبيقات إلى جانب تتبع سلوك المستخدم من أجل تقديم الإعلانات المستهدفة والإعلانات الاجتماعية. وتتمثل مخاطر الإنترنت الرئيسية التي يتعرض لها الطلاب في ثلاثة أنواع، هي مخاطر المحتوى والاتصال والتصرف.

2-2-2 مخاطر المحتوى

تشمل مخاطر المحتوى التي قد تواجه الطلاب الذين تتراوح أعمارهم بين 9 و 12 عامًا أمورًا مزعجة أو مثيرة للاشمئزاز أو غير مريحة، وتشمل الأمثلة على ذلك المواد الإباحية (الصور الفوتوغرافية أو مقاطع الفيديو غير المناسبة) أو عرض صور عن القسوة على الحيوانات أو عنف حقيقي أو عنف المحاكاة. وقد تشمل تلك المواد ما يلي:

- ✓ صور فوتوغرافية أو مقاطع فيديو غير مناسبة
- ✓ عنف حقيقي أو على سبيل المحاكاة
- ✓ مواقع بث الكراهية
- ✓ مواقع المجموعات الإرهابية
- ✓ كما ينشئ المستخدمون محتويٍ ضار مثل المواقع التي تتناول تعاطي المخدرات أو إيذاء النفس أو الانتحار أو صور سلبية لشكل الجسم.
- ✓ التأثيرات التي تم تصميمها لجعل الأفراد يختبرون شعور الصدمة أو الرعب.

2-2-3 مخاطر الاتصال

تشمل هذه المخاطر التواصل مع شخص بالغ يتظاهر بأنه طالب أو التواصل مع شخص غريب يقنع الطالب بمقابلته في الحياة الواقعية أو أن يقع الطالب ضحية للمحتالين عبر الإنترنت، فعلى سبيل المثال، قد يتم إقناع طالبة بمقابلة شخص لا تعرفه (الاستدراج) أو مشاركة معلوماتها الشخصية مع أشخاص غرباء أو تقديم معلومات الاتصال بعد النقر على الرسائل المنبثقة، وغالبًا ما يقوم المتحرشون بإغواء الأطفال من خلال إقامة صداقات قوية عبر الإنترنت وإقامة علاقات عاطفية معهم، حتى لا يعترض الطفل على أي شيء فيما بعد تمهيدًا لإقامة علاقات غير مشروعة مع الأطفال.

2-2-4 مخاطر التصرف

تشمل تلك المخاطر تصرف الطلاب بطرق قد تؤذي الغير، أو وقوعهم ضحايا لهذا النوع من السلوكيات، فعلى سبيل المثال، قد يتلف الطالب لعبة صنعها صديقه أو أحد أشقائه، كما تؤدي مخاطر التصرف أيضًا إلى شراء أشياء غير مناسبة عن طريق الخطأ. وتشمل تلك المخاطر بالنسبة للأطفال الذين تتراوح أعمارهم بين 9 إلى 12 عامًا التصرف بطرق غير مناسبة أو مؤذية أو وقوعهم ضحية لهذا النوع من السلوكيات، وتشمل الأمثلة ما يلي:

- ✓ التسلط عبر الإنترنت
- ✓ الرسائل الإباحية
- ✓ إنشاء محتوى يفصح عن معلومات لأشخاص آخرين
- ✓ مواجهة مشكلات تتمثل في تنظيم قضاء الوقت عبر الإنترنت
- ✓ إساءة استخدام كلمات مرور الأشخاص وانتحال هوية أشخاص عبر الإنترنت
- ✓ القيام بعمليات شراء غير مصرح بها باستخدام تفاصيل مالية لأشخاص آخرين
- ✓ مواجهة مشكلات تتمثل في تنظيم الوقت عبر الإنترنت، والتي يمكن أن تتحول إلى مشكلة تتعلق باستخدام الإنترنت.

2-2-5 تصنيف مخاطر وأضرار استخدام الإنترنت

يختلف تصنيف أنواع المخاطر التي يواجهها الطلاب عبر الإنترنت ودرجة إدراكهم لها، ويعتمد ذلك على كيفية تفاعل الطلاب مع بيئاتهم الرقمية، وبشكل عام، تمثل حوادث المخاطرة عبر الإنترنت مصدر قلق فيما يتعلق بالعدوان والعنف والأضرار الجنسية والمشاكل المرتبطة بالقيم غير المناسبة أو الضارة ومخاطر الإقناع / المخاطر التجارية. ولا يتمثل الهدف من ذلك في إلقاء اللوم على الطلاب لقيامهم بجلب المخاطر بأي طريقة، بل الاعتراف بمجموعة العلاقات المعقدة التي تحدث عبر الإنترنت مع المحتوى ومع أشخاص بالغين ومع طلاب آخرين.

ويوضح الجدول أدناه أمثلة توضيحية والتي ستتغير وتتطور حتماً.

	المحتوى **الطالب كمتلقي** **(الإنتاج الضخم)**	**جهات الاتصال** **الطالب كمشارك** **(أنشطة يمارسها البالغون)**	**التصرف** **الطالب كممثل** **(مذنب/ضحية)**
الاعتداء	محتوى مخيف/عنيف	التحرش والمطاردة	التنمر
التحرش الجنسي	محتوى إباحي	الاستدراج والإساءة الجنسية عند مقابلة الغرباء	الرسائل الإباحية
القيم	محتوى يحض على الكراهية	الإقناع	محتوى يحتمل أن يكون ضار من صنع المستخدم
تجاري	الإعلانات وعمليات التسويق المدمجة	بيانات الموظفين والاستغلال وسوء الاستخدام.	انتهاك حقوق الطبع والنشر والمقامرة

القسم 3: شبكات التواصل الاجتماعي

1-3 مخاطر وسائل التواصل الاجتماعي

1-1-3 المخاطر الشائعة

يمكن أن تشكل مواقع التواصل الاجتماعي مخاطر أيضًا تشمل ما يلي:

- ✓ مشاهدة محتوى غير لائق أو غير مرغوب فيه مثل التعليقات أو الصور العدوانية أو العنيفة أو الجنسية.
- ✓ تحميل محتوى غير لائق مثل الصور المحرجة أو المستفزة أو مقاطع فيديو خاصة به أو بأشخاص آخرين.
- ✓ مشاركة المعلومات الشخصية مع الغرباء، بما في ذلك أرقام الهواتف أو تاريخ الميلاد أو مكان الإقامة.
- ✓ التسلط عبر الإنترنت
- ✓ مشاهدة الكثير من الإعلانات وحملات التسويق المستهدفة
- ✓ اختراق البيانات مثل بيع البيانات إلى مؤسسات أخرى
- ✓ رسائل التطفل في شبكات التواصل الاجتماعي
- ✓ تهديدات الهندسة الاجتماعية
- ✓ التطبيقات والأدوات في شبكات التواصل الاجتماعي
- ✓ تهديدات المحتوى

2-1-3 الأثر الرقمي

يُعرف الأثر الرقمي على أنه مجموعة فريدة من الأنشطة والإجراءات والمساهمات والاتصالات الرقمية التي يمكن تتبعها والتي تظهر على الإنترنت أو على الأجهزة الرقمية، وهي تشمل كل المعلومات التي نتركها وراءنا بعد استخدامنا للإنترنت، بما في ذلك تعليقات وسائل التواصل الاجتماعي ومكالمات سكايب واستخدام التطبيقات وسجلات البريد الإلكتروني، وهذا يعد جزءًا من سجلاتنا على الإنترنت ويمكن رؤيتها من قبل أشخاص آخرين أو تتبعها في قاعدة البيانات، كما يُعرف الأثر الرقمي أيضًا باسم الظل الرقمي والسمعة عبر شبكة الإنترنت والوشم الرقمي، وأيًا كان المسمى فمن الضروري تجاهل الأثر الرقمي، ومع ذلك لا يتم مناقشة هذا الأمر في المنزل أو في الفصل الدراسي كما يجب.

3-2 التنقل بين مخاطر وسائل التواصل الاجتماعي

3-2-1 التحدث إلى الطلاب عن استخدام مواقع التواصل الاجتماعي

يُعد التحدث إلى الطلاب عن استخدام وسائل التواصل الاجتماعي أفضل وسيلة لحمايتهم وضمان سلامتهم على الإنترنت، ويُمثل التحدث فرصة لمساعدة الطلاب على ما يلي:

- ✓ التعرف على الطريقة التي يرغب الطالب في التعامل بها وطريقة تعامل الآخرين معه عبر الإنترنت
- ✓ فهم المخاطر المرتبطة باستخدام وسائل التواصل الاجتماعي - على سبيل المثال وضع علامة عليه في الصور المحرجة التي تم التقاطها في حفلة
- ✓ فهم المخاطر المترتبة بمشاركة محتوى ومعلومات شخصية - وهذا لا يشمل المحتوى الذي يشاركه الطالب فحسب، بل أيضًا صوره التي يشاركها أشخاص آخرون أو المنشورات والصور التي يقوم آخرون بوضع علامة على الطالب فيها.
- ✓ التعرّف على طرق التغلب على المخاطر - على سبيل المثال، إذا قامت طالبة بنشر صورة تحدد شخصها، فيمكنها أن تقلل من المخاطر بعدم تضمين أي معلومات شخصية أخرى
- ✓ تعرّف بما يجب على الطالب فعله في حالة طلب شخص ما معلومات شخصية عبر الإنترنت أو كان مسيئًا أو نشر صورًا محرجة أو شارك معلومات تتعلق بالطالب
- ✓ إدارة الأثر الرقمي للطالب، إذ يمكن على سبيل المثال أن يتحدث المعلم إلى الطلاب عن آثارهم الرقمية في الوقت الحالي وفي المستقبل.

3-2-2 التعرف على القيود العمرية المتعلقة باستخدام وسائل التواصل الاجتماعي

تتغير منصات التواصل الاجتماعي ووظائفها بصورة مستمرة، لذا ينصح بأن تبقى مطلعًا على مستجدات استخدام الطلاب لمواقع التواصل الاجتماعي، ويمكن للمُعلمين طرح أسئلة بشأن المنصات المشهورة والتي يفضل الطلاب استخدامها، كما يمكن أن يطلب المعلمين من أحد الطلاب توضيح طرق استخدامهم لوسائل التواصل الاجتماعي وتحديد ما إذا كانت تلك الوسائل مناسبة من ناحية الفئة العمرية أم لا. ويوجد في بعض منصات التواصل الاجتماعي قيود عمرية، *فعلى سبيل المثال يجب ألا يقل عمر الطالب عن 13 عامًا كي يمتلك حسابًا على فيسبوك وإنستجرام*، وبالرغم من وجود قيود عمرية إلا أنه يصعب تنفيذها نظرًا لقدرة الطلاب على التحايل على الإنترنت بشأن أعمارهم، فيما لا تضع منصات أخرى قيود عمرية معينة، بما في ذلك منصات الألعاب متعددة اللاعبين والتي تسمح للمستخدمين بالتفاعل مع أشخاص آخرين من كافة الأعمار ومن كافة أنحاء العالم. وتملك بعض منصات التواصل الاجتماعي حاليًا إصدارات خاصة بالطلاب، مثل YouTube Student و Messenger Kids. وتطبق تلك المنصات إعدادات أمان مختلفة تتطلب المزيد من التدخل الأبوي وتعرض محتوي مناسب حسب العمر، كما تعرّف تلك المنصات الطلاب بكيفية تصفح وسائل التواصل الاجتماعي.

3-2-3 ماذا عن حظر وسائل التواصل الاجتماعي؟

ازداد مع مرور الوقت اندماج وسائل التواصل الاجتماعي في التطبيقات والألعاب والمواقع الإلكترونية بل وحتى بيئات التعلم؛ لذا يصعب حظرها، كما إنه أصبح من غير العملي حظر أو إغلاق وسائل التواصل الاجتماعي بأي طريقة حتى بالنسبة للطلاب الأصغر سنًا، ولا تعد تلك الطريقة جيدة لتعليم الطلاب طرق التغلب على مخاطر وسائل التواصل الاجتماعي والتعامل باحترام مع أشخاص آخرين. فإذا تم حالة حظر وسائل التواصل الاجتماعي، فقد يميل الطلاب إلى استخدامها في أماكن بعيدة عن المنزل وهو أمر يصعب التحكم فيه.

3-3 الأمان الإلكتروني لوسائل التواصل الاجتماعي

1-3-3 وضع إرشادات تتعلق باستخدام وسائل التواصل الاجتماعي

يمكن أن تساعد الإرشادات المكتوبة الطلاب على استخدام مواقع التواصل الاجتماعي بطريقة تتسم بالمسؤولية والاحترام والأمان. ولكن عندما يستخدم الطلاب وسائل التواصل الاجتماعي في المدارس أو المنازل، فقد يتخلى عن الكثير من الأنشطة المهمة، كالتفاعل والتواصل المباشر بدون تردد، ومن ثم يجب على المعلمين أن يكونوا على دراية بما ينشره الطلاب على الإنترنت إضافة إلى تقديم النصح فيما يخص استخدام مواقع التواصل الاجتماعي في المنزل. وإليكم هنا بعض الإرشادات الموجهة للمعلمين عند تحدثهم إلى الطلاب فيما يخص المخاطر:

1- **ما الذي ينشره الطلاب؟**

التأكد من عدم قيام الطلاب بمشاركة أو نشر:

- ✓ معلومات حساسة: تشمل المعلومات الحساسة أي شيء يساعد أي شخص على سرقة هوية الطالب أو تحديدها، مثل الاسم الكامل وتاريخ الميلاد ورقم التليفون والعنوان ومحل الميلاد...إلخ.
- ✓ المساومة بالمحتوى: يشمل ذلك الصور أو تحديث الحالة بما يلحق الضرر بسمعة الطالب أو تطلعاته المستقبلية.
- ✓ المحتويات القاسية والمزعجة: قد يشمل ذلك كافة الأشياء الضارة الموجهة إلى الطالب أو شخص آخر وكذلك الآراء التي قد يفضل تركها بدون مشاركة.

2- **من هم الأشخاص الذين يتواصل معهم الطلاب؟**

تسمح وسائل التواصل الاجتماعي للطلاب بالتواصل مع أصدقائهم، ولكن توجد مخاطر أيضًا حينما يتواصلون مع أشخاص لا يعرفونهم أو أشخاص يتظاهرون بأنهم أطفال أو حتى مراهقين.

3- **ما هو مستوى الخصوصية الذي يستخدمونه؟**

تتمتع معظم منصات وسائل التواصل الاجتماعي بوجود إعدادات خصوصية تسمح للمستخدمين بتحديد الأشخاص المسموح لهم بمشاهدة المحتوى المنشور، كما توجد إعدادات خاصة بتعقب المواقع والوسم الجغرافي للصور أو الحالات.

4- **التشديد على مفهوم مصداقية الطلاب:**

ليس كل ما ينشر على الإنترنت صحيحًا ويمكن أن يكون الأشخاص الموجودين على الإنترنت غير ما يتظاهرون به.

5- **فكّر في الطريقة التي تعمل بها المواقع الإلكترونية المختلفة قبل الانضمام لها**

تسمح بعض المواقع الإلكترونية لمجموعة محددة من المستخدمين بالوصول إلى المحتوى المنشور، ولكن تسمح مواقع أخرى لأي شخص بمشاهدة تلك المنشورات.

6- **تأكد من عدم إفصاح عن أسمائهم على الشاشة بما يزيد عن ما هو مطلوب**

تجنب استخدام اسمك أو عمرك أو موطنك الأصلي، وحتى إذا فكر المستخدم في أن اسم الشاشة يجعله مجهولاً، فلن يكون الأمر الأمر صعبًا على شخص عبقري في أن يجمع بين العبارات للتعرف على هوية المستخدم وكيفية العثور عليه.

7- استرجاع المعلومات: تذكر إنه بمجرد مشاركة المستخدم معلومات على الإنترنت، فلا يمكن استرجاعها، وحتى في حالة حذف المعلومات من الموقع تظل الإصدارات القديمة باقية على أجهزة الغير.

8- **ويمكن أن تشمل الإرشادات الأساسية ما يلي:**

- ✓ الوقت المسموح فيه بدخول الطلاب إلى وسائل التواصل الاجتماعي ومقدار ذلك الوقت.
- ✓ ما إذا كان يسمح باستخدام وسائل التواصل الاجتماعي خلال أوقات أداء الواجب المنزلي أو تناول الوجبات مع العائلة أم لا.
- ✓ في حالة الاستخدام الضروري لوسائل التواصل - المناطق المدرسية أثناء وقت الراحة.

2-3-3 كيف تؤثر إرشادات استخدام التكنولوجيا على الطلاب

توجه أفعال المعلمين وأقوالهم سلوكيات الطلاب ومعتقداتهم في معظم الأشياء، بما في ذلك استخدام التكنولوجيا، إذ يتأثر الطلاب في المدارس أو المنازل بطريقة استخدام المعلم والأسرة للتكنولوجيا، بل من المرجح أن يحذون حذوهم فيما يفعلونه، فمثلاً هل هاتفك الذكي رفيقك الدائم؟ فعندما يستخدم المعلمون أو الآباء التكنولوجيا في أحيان كثيرة، خاصة وسائل التواصل الاجتماعي، فيمكن أن يتسبب ذلك في التدخل التكنولوجي، ويشير تدخل التكنولوجيا إلى انقطاع تواصلنا وتفاعلنا الشخصي نظرًا لتوجيه انتباهنا نحو الأجهزة الرقمية؛ مما يعني وقوف التكنولوجيا عائقًا في مسار التواصل بين المعلمين والطلاب بل وبين الطلاب وآبائهم.

3-3-3 كن مواطنًا مسؤولاً في العالم الرقمي

أن تصبح مواطنًا مسؤولاً في العالم الرقمي يعني امتلاكك لمهارات اجتماعية إلكترونية تشاركها في الحياة المجتمعية على الإنترنت بطريقة تتسم بالاحترام، مثل:

- ✓ التصرف بطريقة قانونية - إدراك أن التحميل بطريقة غير قانونية هو جريمة مثلاً
- ✓ حماية خصوصيتك وخصوصيات الآخرين
- ✓ إدراك حقوقك ومسؤولياتك عند استخدام وسائل الإعلام الرقمية
- ✓ التفكير في كيفية تأثير الأنشطة الإلكترونية عليك وعلى غيرك وعلى مجتمع الإنترنت الواسع النطاق.

4-3-3 نشر المحتويات والتعليقات

من المهم أن يتفق الطلاب على ما يلي:

- ✓ عدم تحميل أو مشاركة رسائل وصور ومقاطع فيديو عن أنفسهم أو عن الآخرين
- ✓ توخي الحذر فيما يخص المعلومات التي يتم مشاركتها
- ✓ كن مواطنًا مسؤولاً في العالم الرقمي بإظهار الاحترام في المنشورات وعند مشاركة المحتويات، فعلى سبيل المثال عندما يكون من غير المقبول أن تقول شيئًا/ تفعل شيئًا وجها لوجه فلن يكون من الجيد القيام بذلك عبر الإنترنت.

5-3-3 حماية الخصوصية

برزت العديد من المخاوف حول كيفية تعامل منصات تواصل عالمية مثل فيسبوك مع بيانات المستخدمين، لذا يجب مراجعة إرشادات الخصوصية والإعدادات المتعلقة بالطلاب والمشاركة في اتخاذ القرار بشأن المنصات وإعدادات الخصوصية الواجب استخدامها.

يمكن أن يحمي الطلاب خصوصيتهم عن طريق الموافقة على ما يلي:

- ✓ عدم مشاركة معلومات شخصية كأرقام الهواتف ومكان وتاريخ الميلاد مع غرباء أو مع أشخاص لا يعرفونهم شخصيًا
- ✓ عدم إضافة تفاصيل شخصية في ملف التعريف، مثل أرقام الهواتف أو تاريخ الميلاد
- ✓ التحقق من إعدادات الخصوصية والموقع بانتظام، وخاصة على الهواتف المحمولة
- ✓ الاحتفاظ بكلمات المرور ومعلومات الدخول وجعلها سرية وعدم مشاركتها مع الأصدقاء
- ✓ تسجيل الخروج بعد استخدام الحواسيب العامة
- ✓ تعطيل بعض الميزات مثل النشر على العديد من وسائل التواصل الاجتماعي في آن واحد.

3-3-6 البقاء آمنا على وسائل التواصل الاجتماعي

تشمل قواعد السلامة الخاصة بالطلاب ما يلي:

- ✓ حظر الأشخاص غير المعروفين لديهم والإبلاغ عنهم أو أولئك الذين ينشرون تعليقات أو محتويات مزعجة
- ✓ عدم النقر على النوافذ المنبثقة، فقد تبدو بعض النوافذ المنبثقة آمنة لكنها تؤدي إلى مواقع غير لائقة أو تطالبك بتقديم معلومات شخصية أو مالية.
- ✓ قبول طلبات الصداقة من أشخاص يعرفهم الطالب فقط.
- ✓ التقاط لقطة شاشة والتحدث مع شخص بالغ موثوق به بخصوص الأشياء التي يراها الطالب على الإنترنت أو المواقف المزعجة التي قد يواجهها.

3-3-7 إرشادات لإدارة أنشطة وسائل التواصل الاجتماعي

حينما لا يرغب المعلمون في منع الطلاب من المشاركة الاجتماعية سيكون من الجيد إرساء بعض القواعد والإرشادات، تشمل ما يلي:

1- **القيود حسب الأعمار** يفرض فيسبوك قيودًا عمرية على المستخدمين، إذ يجب ألا تقل أعمارهم عن 13 عامًا كي يتمكنوا من إنشاء حساب، ويعد ذلك إرشادًا جيدًا للعديد من منصات التواصل الاجتماعي، مثل تويتر وتمبلر وبنترست.
2- **التواصل مع الآباء/المعلمين:** يجب أن تكون إحدى قواعد التواصل الاجتماعي هي أن يتواصل الطالب مع أحد أبويه أو أحد المعلمين على الموقع.
3- **إعدادات الخصوصية:** لا تحتوي كافة مواقع التواصل الاجتماعي على إعدادات خصوصية، غير أن فيسبوك يطبقها. تأكد من تفعيل إعدادات الطالب بحيث يتمكن الأصدقاء فقط من مشاهدة المنشورات وليس العامة.
4- **الاستخدام المقنن:** تتمثل إحدى إشارات تعرض الطالب للتنمر عبر الإنترنت في بقاؤه متصلاً بالإنترنت لوقت طويل للغاية، لا سيما موقع التواصل الاجتماعي المستخدم للهجوم، لذا يجب أن تكون ملمًا بالمواقع التي يدخلون إليها ومدة بقاؤهم هناك ونشاطهم العام على الإنترنت.
5- **التوعية بعواقب استخدام الإنترنت ومخاطره:** من المهم أن يدرك الطالب عواقب المشاركة الإلكترونية، لذا عليك أن تحثهم بالتفكير طويلاً ومليًا قبل أن ينشروا أي شيء، كما عليك أن تحثهم على عدم إعطاء معلومات شخصية وتعرفهم بطريقة التعامل مع التعليقات غير المهذبة أو المهينة الصادرة عن الآخرين، إلى جانب تعريفهم بكيفية حظر الأشخاص حتى لا يضطروا إلى التعامل مع التعليقات غير اللائقة.
6- **كن قدوة يحتذى بها:** في حالة تواصل المعلمين والطلاب عبر وسائل التواصل الاجتماعي، فسيتمكنوا من مشاهدة منشوراتك أيضًا، وهو ما يعني وجود حدود للاحترام، كما يجب تجنب نشر أشياء غير لائقة. وعليك الاتسام بالإيجابية والتأكد من كون أنشطتك آمنة، إذ يلجأ الطلاب إلى البالغين لطلب التوجيه والدعم ويشمل ذلك استخدامهم للإنترنت.

3-4 ما الذي يتعين على المعلمين معرفته بشأن أحدث تطبيقات وسائل التواصل الاجتماعي الخطيرة

3-4-1 تطبيقات وسائل التواصل الاجتماعي التي يجب أن يطلع المعلمون عليها

يتم إطلاق تطبيقات تواصل اجتماعي جديدة يوميًا؛ لذا يصعب أن يبقى المعلمين / الآباء على اطلاع وتحديد التطبيقات الأكثر أمانًا والأكثر خطورة، لذا لم تعد مواقع تويتر أو سناب شات والإنستجرام هي المنصات الوحيدة التي تثير قلق المعلمين والآباء، لذا يجب أن يتعرف المعلمين كلهم على تطبيقات التواصل الاجتماعي الأربعة التالية:

1- **بلندر**: تم تصميم هذا التطبيق للدردشة بين البالغين ومقابلة أناس جدد، وعلى الرغم من وجود مطلب للتسجيل وهو أن لا يقل سن المستخدم عن 18 عامًا فقد وجد الطلاب حيلة لاستخدامه، وبمجرد قيام الطالب بإنشاء ملف شخصي عن طريق إضافة صور و/أو مقاطع فيديو وكذلك موقع معيشته، فهو يملك حرية التنقل وفقًا لاهتماماته بملف تعريفي محدد. وتتمثل المخاطر الواجب أن يكون الآباء على دراية بها فيما يلي:

- ✓ سهولة التحايل على القيود العمرية نظرًا لعدم طلب بطاقة تحقيق شخصية.
- ✓ يمكن أن يتظاهر البالغين بأنهم مراهقون والعكس بالعكس.
- ✓ تزيد مشاركة الموقع من احتمالية إجراء مقابلات شخصية.
- ✓ يمكن أن يشارك المستخدمين صورًا فاضحة.
- ✓ قد يختار المستخدمون ربط التطبيق بحساباتهم على فيسبوك وجوجل بلس وإنستجرام وتويتر ولينكد وهو ما يقلل من فرص بقاؤهم مجهولي الهوية.

2- **كالكيلاتورز:** يطلق عليه أيضًا "تطبيق الآلات الحاسبة السرية أو الزائفة" إضافة إلى تطبيق "فوتو فالوتس"، حيث يُمكن هذا التطبيق من إخفاء الصور والملفات في تطبيق يشبه آلة حاسبة نمطية، وتشمل المخاطر ما يلي:

- ✓ سهولة إخفاء الطلاب للصور والفيديوهات والنصوص ومتصفحات الويب بل وحتى جهات الاتصال.

3- **لايف مي:** يعد Live.me تطبيق بث مباشر مصمم من للقيام بعمليات "البث والدردشة والمشاركة والمتابعة وأن تكون نجمًا!" كما يتمكن المراهقين من بث فيديوهات مباشرة ومشاهدة فيديوهات الآخرين، وتنص شروط الاستخدام على ألا يقل سن المستخدم عن 13 عامًا، ومع ذلك يستخدمه طلاب أصغر سنًا، ولكن يترتب على استخدامه مخاطر أيضًا تشمل ما يلي:

- ✓ يشارك المستخدمون مواقعهم مع إمكانية التعرف على الأشخاص الذين يبثون فيديوهات في النطاق المحلي مما يزيد من احتمالية إجراء لقاء شخصي.
- ✓ لا يمتلك المستخدمون خصوصية نظرًا لعدم إمكانية مراقبة الأشخاص الذي يشاهدون البث الخاص بهم.
- ✓ يتم استدراج بعض الفتيات القاصرات من قبل أشخاص ذوي ميل جنسي للأطفال للقيام بممارسات جنسية.
- ✓ يتم تسجيل عمليات البث عن طريق مستخدمين بدون معرفة الطلاب ومن ثم نشرها في مواقع أخرى.
- ✓ توجد إمكانية لنشر تعليقات جارحة وتنمر منتجي البث.

4- **يوبو:** أطلق على تطبيق يوبو سابقًا اسم "يولو": كوّن صداقات جديدة" وهو تطبيق مصمم من أجل الدردشة ومتابعة الأشخاص بعضهم البعض عن طريق مواقع إنستجرام وسناب شات، حيث يجب ألا يقل عمر الشخص المتقدم للتسجيل عن 13 عامًا، ويمكن للمستخدمين الذين تقل أعمارهم عن 18 عامًا إجراء محادثات مع أشخاص تتراوح أعمارهم بين 13 و17 عام فقط، أما المستخدمين الذين تتجاوز أعمارهم 18 عامًا فيمكنهم إجراء محادثات مع أشخاص في سنهم أو أكبر منهم، كما يتمكن مستخدمو يوبو من إنشاء ملف تعريفي بإضافة صور ومقاطع فيديو واستخدام روابط إنستجرام وسناب شات، وتشمل المخاطر ما يلي:

- ✓ سهولة تحايل الطلاب على القيود المفروضة على العمر لعدم إلزامهم بتقديم بطاقة تحقيق الهوية.
- ✓ يمكن أن يتظاهر البالغين بأنهم مراهقون والعكس بالعكس.
- ✓ تزيد مشاركة الموقع من احتمالية إجراء مقابلات شخصية.
- ✓ يقوم المستخدمون بإجراء ربط تلقائي بحسابات سناب شات وإنستجرام خاصة بأناس آخرون وهو ما يقلل من فرص بقاؤهم مجهولي الهوية.



القسم 4: المخاطر والأضرار الإلكترونية

4-1 التنمر والاعتداء والكراهية

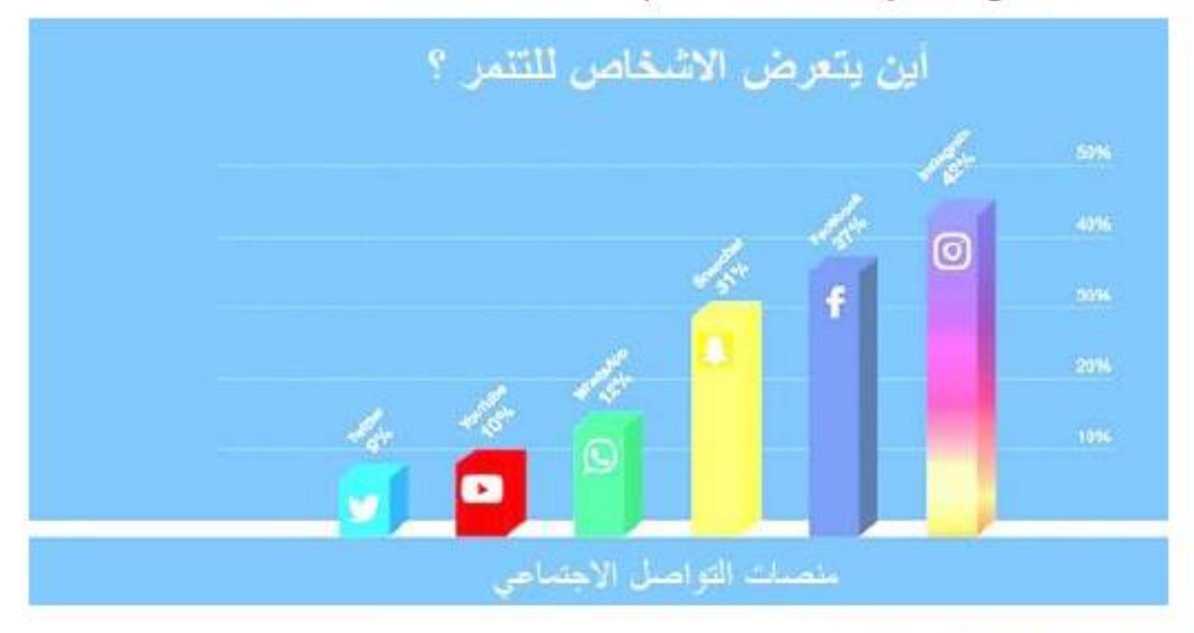
4-1-1 ما هو مفهوم التنمر؟

يحدث التنمر عندما يقصد شخص ما وبصورة متكررة إخافة أو تهديد أو إيذاء شخصًا آخر أو ممتلكاته أو سمعته أو وضعه الاجتماعي، أما التنمر على الإنترنت فيعني التصرف بوقاحة أو بدء صراع على الإنترنت بدون سبب واضح.

يمكن تعريف التنمر بما يلي:

- ✓ **التنمر اللفظي:** الإهانة أو التهديد أو السخرية من شخص معين
- ✓ **التنمر السري دون علم شخص ما:** المزاح واستخدام ألفاظ سيئة أو نشر إشاعات أو تشجيع الأقران على استبعاد شخص ما.
- ✓ **التنمر الجسدي:** الدفع أو الإيذاء أو الضرب أو إلحاق الضرر بالممتلكات
- ✓ **التنمر على الإنترنت:** استخدام التقنيات الرقمية للتحرش أو المضايقة المتعمدة (المناقشة الرئيسية)

حيث تتسبب شتى أنواع التنمر في حدوث أذى ولكن يؤدي استمرارها إلى أضرار طويلة الأمد.



4-1-2 التنمر على الإنترنت - الشرح

يستخدم التنمر على الإنترنت تقنيات رقمية بغرض إيذاء شخص معين، ويحدث التنمر على الإنترنت عندما يستخدم شخص ما تقنيات رقمية لمضايقة شخص آخر أو إهانته أو إحراجه أو التعدي عليه أو تهديده أو السخرية منه أو ترويعه. ويحدث التنمر على الإنترنت عندما يقوم شاب ما بالتحدث عن شخص آخر أو مجموعة من الطلاب بطريقة سلبية على الإنترنت، ويمكن أن يشمل ذلك مضايقة شخص معين أو تهديده أو حتى تشويه سمعته عن طريق نشر الأكاذيب. وعند استخدام مواقع التواصل الاجتماعي مثل فيسبوك، يسهل تنمر الطلاب ببعضهم في بيئة الإنترنت، وعادة ما تتكرر محاولات التنمر على الإنترنت، وهي تنطوي في كثير من الأحيان على تبادل الكثير من الرسائل بين الأطراف المُنخرطة، ويمكن أن يتم إرسال تلك الرسائل

باستخدام أحد برامج المراسلات الفورية، مثل ياهو! كما يمكن كتابة مدونات سلبية عن مراهقين ليسوا على دراية بأنشطة التشهير، ولذلك يظل التنمر مرتبطًا بالطلاب فقط، ولكن حينما يتورط شخص بالغ يتحول الأمر إلى مطاردة وتحرش إلكتروني، وتساعد معرفة أشكال التنمر على الإنترنت وما يتعلق بها في إيقاف تعرض الطلاب لهذا الشكل من التنمر، لذا يجب أن يناقش المعلمون التنمر على الإنترنت وعواقبه على الطلاب حتى لا يتعرضوا هم أنفسهم للتنمر على الإنترنت. ويمثل الوعي ركيزة أساسية لمنع وقوع أي حوادث وضمان عدم تحول الطلاب إلى ضحايا.

يحدث التنمر على الإنترنت **في أي وقت من الليل أو النهار** وفي أي مكان تتوفر فيها سبل الوصول على الإنترنت. ويجب أن يتابع المعلمون الطلاب ذوي الإعاقة (الاحتياجات الخاصة)؛ إذ يمكن أن تؤدي الإعاقة إلى سهولة تعرضهم للتنمر.

4-1-3 أسباب حدوث التنمر على الإنترنت

يقع الطلاب في فخ التنمر على الإنترنت لأسباب عديدة ومختلفة، فربما يكونوا قد شاهدوا سلوكيات عدوانية في المنزل أو في أي مكان آخر أو ربما تعلموا التعصب تجاه مجموعات معينة، أو ربما تعرضوا لإساءة بدنية أو عاطفية، علاوة على ذلك، عندما يلتحق الطلاب بالمدارس الثانوية فإنهم يبحثون عن طرق تزيد من تأثيرهم وأهميتهم الاجتماعية، لذلك قد يتسمون بالقسوة أو استبعاد الآخرين، ويمكن أن يحدث التنمر أيضًا في الصداقات السامة، ويتمثل ذلك في سخرية الطلاب من أحد أفراد المجموعة أو استبعاده، ويتسم هذا السلوك بالمكر في أغلب الأحيان؛ لذا يمكن أن يشعر الطلاب الخاضعون للتنمر بأنهم في غاية الارتباك بسبب ما يحدث.

4-1-4 عوامل الخطورة

تم تحديد مجموعة واسعة من التنبؤات المتعلقة بتلك السلوكيات، فعلي سبيل المثال حددت التقييمات الأخيرة الغضب والسلوك الخطر على الإنترنت بوصفها عوامل مخاطرة تسبب الإيذاء والتعرض للتنمر على الإنترنت والمعتقدات المعيارية المتعلقة بالعدوان باعتبارها تنبئ بارتكابه، ولا ينظر الكثير من المراهقين إلى عواقب تلك المشكلة ولا يدركون أنهم يقحمون أنفسهم في تهمة جنائية محتملة، هذا في الوقت الذي لا يدرك فيه البعض أو لا يكترثون إلى أنهم يضرون بسمعة أناس آخرين، ويسببون الاكتئاب للبعض الآخر، حيث يجعل التنمر على الإنترنت الطلاب يشعرون بعدم الثقة بالنفس، وينخفض اهتمامهم بالمدرسة، وتنخفض معدلات الإنجاز الأكاديمي لديهم، وقد ينتهي الأمر بالطلاب الذي عاشوا التنمر على الإنترنت إلى أن يتعرضوا للتنمر في بيئة المدرسة، وقد يشعر الطلاب بالارتباك بسبب تغير مجموعات الأصدقاء الخاصة بهم، وقد يشعرون أيضًا بالوحدة والعزلة، وقد يترتب على التنمر على الإنترنت مشكلات عقلية، كالاكتئاب والقلق والضغط بل قد يؤدي في الحالات القصوى إلى الانتحار، ويشعر بعض ضحايا التنمر على الإنترنت بعدم امتلاكهم لمكان آمن.

4-1-5 ما هي الأشياء التي يحتاج المعلمون معرفتها

يحدث التنمر على الإنترنت بعدة طرق مختلفة؛ عن طريق الهواتف المحمولة والرسائل النصية ورسائل البريد الإلكتروني ومن خلال مواقع الألعاب والتواصل الاجتماعي، مثل فيسبوك ويوتيوب وإنستجرام. **أمثلة على حالات التنمر على الإنترنت:**

- ✓ نشر أو إرسال رسائل تهدد أشخاص أو تجعلهم في موقف سيئ
- ✓ استبعاد أشخاص من مواقع الألعاب أو المنتديات الاجتماعية
- ✓ نشر شائعات سيئة عن أشخاص عبر الإنترنت
- ✓ إنشاء حسابات مزيفة أو مزعجة على مواقع التواصل الاجتماعي باستخدام صور حقيقية ومعلومات الاتصال بالضحية
- ✓ تعقب الآخرين عبر الإنترنت
- ✓ مشاركة أو إعادة توجيه معلومات تخص أشخاص آخرين
- ✓ نشر شتائم أو صور مخلة أو فيديوهات عن أشخاص
- ✓ مضايقة الآخرين في البيئات الافتراضية أو ألعاب الإنترنت

4-1-6 المعلمون: علامات التعرف على العلامات

عادة ما يصعب اكتشاف التنمر على الإنترنت بين المراهقين مقارنة بالتنمر بين الطلاب الأصغر سنًا، وقد يسعى بعض الطلاب إلى إخفاء هذا التنمر عن معلميهم وأبائهم، فقد يشعر الطالب بالخجل والخوف أو ربما لا يرغب في إزعاجك أو أن تشعر بوجود مشكلة كبيرة، وعادة ما يرغب الطلاب في إنهاء حالة التنمر دون الالتفات له، ولكن توجد بعض إشارات التنمر والتي يجب أن يلاحظها المعلمون، فعلى سبيل المثال قد يواجه الطلاب المعرضون للتنمر مشكلات في المدرسة أو يظهرون إشارات عاطفية أو جسدية.

1- **المشكلات الأكاديمية:**

- ✓ يأخذ التنمر على الإنترنت أشكال عدة، ولذلك تختلف الإشارات الأولى اختلافًا كبيرًا، وقد يكون بعضًا من تلك الإشارات الأولى متعلقًا بالناحية الأكاديمية: فربما يتحول طالب اعتاد على الحصول على تقييم A إلى طالب يحصل على علامات متدنية أو طالب كان متحمسًا للذهاب إلى المدرسة إلى طالب يختلق الأعذار كي لا يذهب إليها.
- ✓ وقد يواجه الطالب الذي تعرض لتنمر على الإنترنت مشكلات من خلال بدء العراك مع طلاب آخرين أو الرد بقلة احترام على رموز سلطوية. وسواء كان السبب تنمر على الإنترنت أو شي آخر يجب على المعلمين توخي الحذر.

2- **قد يفقد ضحايا التنمر على الإنترنت اهتمامهم** بالأنشطة التي كانوا يستمتعون بأدائها بها في السابق أو قد يغيرون العادات الغذائية الخاصة بهم، وقد يتوقفون عن استخدام الأجهزة الرقمية وإغلاق حساباتهم الإلكترونية.

3- **التغيب عن المدرسة:** غالبًا ما يمتنع الطلاب الذين تعرضوا للتنمر على الإنترنت عن الذهاب إلى المدرسة حيث يواجهون المتنمرين وأقرانهم، وفي حالة تظاهر طالب بالمرض في حالات عديدة، فقد يكون السبب في ذلك هو عدم رغبته في الذهاب إلى المدرسة، وقد يكون مريضًا بالفعل لأن القلق والضغط يؤديان إلى في ظهور أعراض مثل ألم المعدة والصداع.

4- **العزلة والشعور السيء:** قد يدفع التعرض للتنمر على الإنترنت (أو التنمر في الحياة العادية) إلى انسحاب الطالب من الحياة الاجتماعية، وفي حالة قضاء الطالب الكثير من الوقت وحيدًا في غرفته، فمن المحتمل أن يكون قد تعرض للتنمر، لذا يجب النظر في مقدار الوقت الذي يقضيه الطالب على الإنترنت، وفي حالة اتصاله الدائم بمواقع التواصل الاجتماعي، فمن المحتمل إنه يقرأ منشورات التنمر والتعليقات المتعلقة به.

5- **تغير العادات:** ليس من غير المألوف أن يغير الطالب عاداته ردًا على التنمر على الإنترنت.

6- **السلوكيات المدمرة للذات:** قد يلجأ الطلاب إلى سلوكيات مدمرة للذات في حالة استمرار التنمر على الإنترنت، فيمكن أن ينتهجوا نهجًا غير أخلاقيًا أو يتحولوا إلى تناول المخدرات أو الكحول أو البدء في الإضرار بأنفسهم، وفي بعض المواقف، يحاول الطالب / الطالبة التخلص من حياتهم في محاولة للهرب من ضغوط التنمر على الإنترنت.

7-1-4 مساعدة الطلاب في تجنب التنمر على الإنترنت

يرد فيما يلي بعض الأشياء التي يمكنك القيام بها للمساعدة في تقليل تعرض الطلاب للتنمر على الإنترنت:

1- **الموافقة على القواعد:** يمكن أن تساعد الموافقة على قواعد واضحة فيما يتعلق بأوقات استخدام الطلاب لهواتفهم المحمولة أو أجهزة الكمبيوتر أو الكمبيوتر اللوحي في تقليل فرص التنمر على الإنترنت، فعلى سبيل المثال غالبًا ما تحدث التنمر على الإنترنت في أوقات الليل عن طريق الرسائل النصية ومشاركة الصور، ومن المستحسن أن يوقف الطالب تشغيل جميع الأجهزة في فترة الليل وتركها في منطقة العائلة.

2- **التحدث إلى الطلاب عن التنمر على الإنترنت:** من الجيد أن تبدأ الحديث عن التنمر على الإنترنت عندما يبدأ الطالب في استخدام مواقع التواصل الاجتماعي، أو عندما يحصل على هاتف محمول.

3- **تحدث عن:**

- ✓ **توصيف التنمر على الإنترنت:** وضح أن التنمر على الإنترنت يتمثل في إرسال رسائل نصية تحوي عبارات مشينة أو نشر الشائعات على وسائل التواصل الاجتماعي أو التسلط الجماعي على لاعب في لعبة على الإنترنت أو مشاركة صورة محرجة مع أشخاص آخرين.
- ✓ **ما هو شعور الشخص الذي تعرض لتنمر على الإنترنت:** ناقش كيف يمكن أن يؤدي التعرض للتنمر إلى الشعور بالضيق والوحدة، فقد يمتنع الطالب عن المشاركة في الأنشطة التي قد يحدث فيها تنمرا.
- ✓ **عواقب التنمر على الإنترنت:** اشرح كيف يمكن أن يتراجع المستوى الدراسي الطلاب الذين تعرضوا لتنمر على الإنترنت إضافة إلى شعورهم بالاكتئاب أو القلق.
- ✓ تحدث عن الأمان عبر الإنترنت.

4- **قد يشمل هذا الحديث عن أشياء مثل:**

- ✓ **الأصدقاء عبر الإنترنت وقوائم أصدقاء المراسلة:** إذا أضاف الطالب شخصًا لا يعرفه حقًا "كزميل" أو "صديق"، فهو يمنح هذا الشخص حق الوصول إلى معلومات خاصة به وبالتالي استخدامها لممارسة التنمر على الإنترنت.
- ✓ **عدم إعطاء كلمات المرور للأصدقاء:** يعطي بعض الطلاب كلمات المرور لأصدقائهم في إشارة للثقة، ولكن كلمات المرور تمنح الآخرين القدرة على انتحال شخصية الطالب على الإنترنت.
- ✓ **التفكير قبل النشر:** إذا قامت طالبة بنشر تعليقات شخصية أو صور أو مقاطع فيديو، فمن المحتمل أن تحصل على اهتمام غير مرغوب فيه أو تعليقات سلبية، ويمكن أيضًا أن تظل التعليقات والصور متاحة عبر الإنترنت لفترة طويلة.
- ✓ **إخبار شخص بالغ:** تحدث إلى أحد المعلمين أو شخص بالغ موثوق به في حالة الشعور بالقلق حيال أي شيء يحدث عبر الإنترنت.

8-1-4 تقديم الدعم للطالب الذي تعرض للتنمر

إذا تعرض الطالب للتنمر عبر الإنترنت، فمن الجيد أن يشعر بأن لديه قدرة تمكنه من حل المشكلة بنفسه، وتساعد الخطوات الست التالية في **التخلص من** التنمر على الإنترنت، وقد يتطلب الأمر قيام المعلم بمساعدة الطالب للتعرف على تلك الخطوات والإبلاغ عن حوادث التنمر على الإنترنت. وقد يؤدي تقديم الدعم في إحداث فرق، حيث يشعر بعض الطلاب بأنهم منهكون عاطفيًا بدرجة تجعلهم غير قادرين على الإبلاغ عن الحوادث بأنفسهم.

1- G **-حجب الشخص المشارك في التنمر على الإنترنت أو حذفه:** يساعد حظر شخص ما من قائمة الأصدقاء في منعه من الانخراط في التنمر على الإنترنت ومن نشر أو تحميل محتوى مسيء عن الطالب، وفي حالة حدوث التنمر من خلال الرسائل النصية أو المكالمات الهاتفية، فيمكنك أن تطلب من مزود الخدمة مراقبة المكالمات أو النصوص، وقد يتصل مزود الخدمة بالمرسل إذا لزم الأمر، لقيام حامل الهاتف المحمول بخرق العقد المبرم بينه وبين الشركة بسبب استخدام هاتفه في التنمر. كما يمكنك تغيير رقم هاتفك إذا لزم الأمر.

2- E **– التأكد من الاحتفاظ بدليل على التنمر**: يجب أن تحتفظ بأي من رسائل التنمر وتقوم بطباعتها. واستخدم مفتاح شاشة الطباعة أو الأمر الموجود على لوحة مفاتيح الكمبيوتر، ويمكن أن يقوم الطالب أيضًا بأخذ لقطة من شاشة الهاتف المحمول.

3- T **-أخبر شخص ما**: تساعد مشاركة الطالب مشاعره مع أحد أبويه أو أخوه الأكبر أو الأقارب أو المعلم أو صديقه المقرب في أقرب وقت ممكن في إزالة شعوره بالعزلة.

4- R **– الإبلاغ عن الإساءة**: قد تكون هناك عواقب على الشخص المنخرط في التنمر إذا تم الإبلاغ عن الإساءة، ويمكن أن يطلع المعلمين والطلاب على مواقع التواصل الاجتماعي معًا للتأكد من معرفة الطالب لكيفية الإبلاغ عن الإساءة.

5- I – **بدء السيطرة:** عندما يسيطر الطالب على التنمر على الإنترنت يمكنه أن يشعر بالأمان والخروج من تلك الحلقة المفرغة، ويتمثل الجزء الأكبر من السيطرة في الإبلاغ عن الإساءة، لا **الانتقام أو الرد بعنف** على التنمر على الإنترنت، فمن الأفضل ألا يتعامل الطالب مع المتنمر على الإطلاق، إذ يمكن للانتقام أو حتى إبلاغ المتنمر بالتوقف أن يجعل وضع التنمر أكثر سوءًا.

6- D– **حذف الرسائل المتعلقة بالتنمر**: بعد حفظ أدلة التنمر، قم بحذف الرسائل والمنشورات. **لا تقم بإعادة توجيه الرسائل أو إعادة نشرها أو إعادة نشر التغريدة أو إرسالها** إلى أشخاص آخرين بأي طريقة؛ لأنهم قد يقوموا بإعادة إرسالها أيضًا.

9-1-4 دور الآباء في دعم الطلاب في المنزل

يرد هنا بعض الأفكار المتعلقة بدعم الطلاب في المنزل:

- ✓ **أظهر للطلاب الكثير من الرعاية والحب:** يمكنك إظهار الحب بطريقة تتناسب مع عمر الطالب ودرجة نضجه، وقد يكون ذلك في صورة احتضان أو رَبْت على الكتف أو إخباره بأنك تهتم به.
- ✓ **الاستماع الإيجابي:** تأكد من الاستماع إلى ما يشعر به الطالب: ناقش كيف يمكن استبعاد الطالب من الكثير من الأنشطة وكيف يؤثر ذلك عليه سلبًا.
- ✓ أخبر الطالب بأن التنمر لن يستمر للأبد: أخبر الطالب بأن الأمور ستتحسن وناقش الموقف بصراحة في أي وقت يختاره الطالب.
- ✓ تأكد من أن الطالب يدرك أن التنمر ليس خطئه: إذ يحتاج الطالب إلى معرفة إنه لم يرتكب أي خطأ. وناقش حقيقة أن الأمر لن يكون على ما يرام إذا تعامل شخص آخر مع الطالب بهذه الطريقة. وحدد الصفات الجيدة التي يمتلكها هذا الطالب.
- ✓ **وجّه الطالب خلال المشكلة:** اذكر للطالب كيف يمكن أن يساعد التحدث عن الموقف في تحسين الأمور وناقش الأفكار.
- ✓ **ساعد الطالب في التعرف على الأماكن الآمنة/الأشخاص الداعمين:** وضح للطالب المناطق الآمنة التي يمكنه الذهاب إليها مثل المكتبة، استخدم الخريطة المدرسية لإيجاد الأماكن الآمنة. ابحث عن البالغين الداعمين في المدرسة وعرف الطالب بأسماء ثلاثة منهم للبحث عنهم عند وجود مشكلة.

4-1-10 العمل مع مدرسة الطالب لحل مشكلة التنمر

عندما يتعرض الطالب للتنمر داخل المدرسة فمن المهم أن تتدخل المدرسة في أسرع وقت ممكن، إذ يجب على المدارس أن تأخذ هذه المشكلة بجدية، فيمكنها العمل مع المعلمين في محاولة لمنع تزايد هذه المشكلة. فيما يلي كيفية إشراك المدرسة بطريقة إيجابية وبناءة:

- ✓ دع الطالب يعرف أنك ستشرك المدرسة في المشكلة. حاول أن تكتشف إذا ما كان الطالب يرغب في الحضور أثناء مناقشة هذا الأمر وإذا أراد المشاركة.
- ✓ حدد موعدًا لمقابلة معلم الطالب أو المنسق العام أو رئيس قسم العناية الرعوية.
- ✓ ناقش المشكلة مع ممثلي المدرسة واطرح الحقائق المعروفة ثم اطلب رأي المدرسة.
- ✓ كن حازمًا وليس غاضبًا وكن مستعدًا للاستماع.
- ✓ اطلب نسخة من سياسة المدرسة في التعامل مع مثل هذه المشكلة واسألهم كيف سيتم تطبيقها على هذا الموقف.
- ✓ انه الاجتماع بخطة لكيفية إدارة الموقف ووقت اجتماع المتابعة.

4-1-11 عند رغبة الطالب في عدم إشراك المدرسة في المشكلة

قد يشعر الطالب بالإحراج أو القلق من أن مشاركة المدرسة سيجعل الأمر أسوأ، لذا من المهم أن تستمع إلى اهتمامات الطلاب ومحاولة فعل أي شيء للتقليل من قلقه/قلقها. فعلى سبيل المثال، قد تكون قادرًا على تحديد موعد في المدرسة في وقت يقل فيه احتمالية ملاحظة الطلاب الآخرين، لكن في النهاية، يكون الأشخاص البالغين هم أفضل مَن يقرر مصلحة الطالب حتى لو كان ذلك يعني إشراك المدرسة ضد رغباته.

4-1-12 ماذا تفعل إذا استمر التنمر

في حالة استمرار المشكلة، فهذا يعني أن التعاون مع المدرسة لا يزال هو الحل الأفضل بدلاً بل تحمل المسؤولية منفردًا، وفي هذه المرحلة، من المهم أن يكون لديك سجلاً بما يحدث، لذا، عندما يكون هناك حادثة تنمر، ينبغي أن يسجل الطالب ما يلي:

- ✓ ماذا حدث بالضبط
- ✓ اسم/أسماء الشخص / الأشخاص الذين قاموا بهذا الفعل
- ✓ متى وأين حدث ذلك الفعل
- ✓ ما قاله الطالب أو فعله لمحاولة منع ذلك التصرف

في حالة اشتمل التنمر على إيذاء جسدي، فينبغي على الطالب أن يلتقط صورًا لذلك. يمكن أن يأخذ الطالب **لقطات الشاشة** إذا كان التنمر يتضمن وضع منشورات على مواقع التواصل الاجتماعي أو تعليقات على رسائل الدردشة الفورية أو رسائل البريد الإلكتروني أو الرسائل النصية. يمكن أن يعطي الطالب نسخة من هذا التسجيل للمعلم الذي يثق فيه لتقديم المساعدة. وهنا يتطلب الأمر مشاركة المدرسة مرة أخرى ويمكن أن يقدم الطالب دليلاً بالحادثة والجدول الزمني المرتبط بها. وفي هذه المرحلة، يجب تناول الحادث كتابة، وسيتعين إشراك مدير المدرسة أو مجلس إدارتها في حالات التنمر الخطيرة. وفي حالة اتخاذ إجراء غير مرضٍ، فقد يطلب ولي أمر الطالب مراجعة إجراءات التظلم بالمدرسة.



13-1-4 الصديق العدو والصداقات السامة - ما تحتاج إلى معرفته



الصديق العدو هو الشخص الذي يبدو ودودًا بالرغم من إنه يخفي كرهًا أو صراع كبير داخله، إذ يمكن أن تتحول الصداقات الطلابية إلى علاقات سامة أو تتطور إلى أبعد من ذلك إذا تسكع الطالب مع أعداء يتظاهرون بأنهم أصدقاء، فوجود مثل هذا النوع من الطلاب يعني بالضرورة تعرض الطالب للتنمر. فبدلًا من جعل الطالب يشعر بالرضا والقبول والانتماء يمكن أن تؤدي الصداقات السامة إلى جعل الطالب يختبر مشاعر سلبية تجاه نفسه أو تجاه الآخرين، وذلك لأن الأصدقاء المزيفين غالبًا ما يحبطون أقرانهم أو يتلاعبون بهم أو يتركونهم أو يتصرفون بطرق مسيئة أخرى. تظهر الصداقات السامة كأنها صداقات طبيعية في البداية، لكن بمرور الوقت سيتصرف الطالب بطريقة معينة تظهر وجهه الحقيقي. راقب التغيرات السلوكية لتحديد الصداقات السامة. إليك بضعة أسئلة لمساعدتك في تحديد إذا ما كان هناك مشكلة:

1- هل تخلى الطالب عن أشياء كانت مهمة بالنسبة له لإرضاء هذا الصديق؟
2- هل يخرج الطالب مع شخص واحد فقط بعدما كان يخرج مع عدة أصدقاء؟
3- هل هذه العلاقة عادت / انقطعت مرة أخرى؟ هل هم أصدقاء لمدة أسبوع واحد وليس لأسبوع آخر؟
4- هل يختلق المراهق الأعذار لسلوكيات صديقه السيئة؟

ونتيجة للصداقات السامة قد يشعر الطالب بتدني الذات، وقد يشعر إنه لا يستحق أصدقاء آخرين، لذا يعتمد على الأصدقاء المزيفين ليشعر بالتقدير.

2-4 الإعلان والطلاب

يرى الطلاب إعلانات كل يوم. وتعد القدرة على فهم ما تحاول الإعلانات تقديمه ماهرة حياتية مهمة وقد يساعد المعلمون الطلاب على تطويرها.

1-2-4 ما يحتاج المعلمون لمعرفته عن الإعلانات على الإنترنت

تجربة الطلاب في الإعلان بأشكال عديدة- على التليفزيون واليوتيوب والتطبيقات والراديو واللوحات الإعلانية والمجلات والجرائد والأفلام والإنترنت والرسائل النصية ووسائل التواصل الاجتماعي والمزيد، فهذه الأنواع من الأعمال الإعلانية تستهدف الطلاب. فعلى سبيل المثال، كلما ازداد عدد الطلاب الذين يشاهدون التليفزيون، زاد عدد الألعاب التي قد يرغب الطلاب في شراءها، لذا، فمن المهم أن يدرك الطالب أن الإعلانات تدفعه لشراء شيء ما، إضافة إلى تأثيرها على طريقة تفكير الأطفال وتغيير آرائهم بشأن بعض الأشياء، إذ يتمثل هدف المعلنون في جعل منتجاتهم تبدو مذهلة، وربما أفضل مما هي عليه حقًا. **ولاشك أن الإعلان يؤثر على الطلاب بطرق مختلفة،** إذ يمكن أن تعتمد طريقة تفاعل الطلاب مع الإعلانات على عوامل عدة، بما في ذلك أعمارهم وما يعرفونه وما اختبروه وعدد الفرص التي طرحت عليهم وما يشاهدونه في وسائل الإعلام. ويشير مصطلح ألعاب الإعلان إلى الألعاب المستخدمة للإعلان عن علامة تجارية أو منتج ما، فعلى سبيل المثال، قد تتضمن اللعبة البحث عن شخصية تجلب حلويات تحمل علامة تجارية ترعاها الشركة.

2-2-4 كيف يمكن للطالب تحديد الإعلانات

بناء على عمر الطالب:

الأعمار أقل من 7 سنوات:

- ✓ يمكنهم تحديد الإعلانات وتمييزها من البرامج، ولكنهم لا يدركون أن الإعلانات تحاول بيع شئ ما.
- ✓ يميلون إلى اعتبار الإعلانات مواد ترفيهية أو إشعارات مفيدة
- ✓ لن ينتقدون الإدعاءات التي يقدمها المعلنون

الأعمار من 7-11 سنة :

- ✓ يدركون أن الإعلانات تحاول بيع شئ ما
- ✓ يمكنهم تذكر الرسائل الإعلانية
- ✓ يمكنهم إدراك بعض تقنيات الإعلان مثل الإعلانات المبالغ فيها فيما يخص جودة المنتجات
- ✓ لا يمكنهم حماية أنفسهم دائمًا عن طريق طرح أسئلة عما تفعله الإعلانات
- ✓ قد لا يفهمون دائمًا أن المنتجات ليست جيدة كما تبدو

3-2-4 الحد من آثار الإعلان على الطلاب في سن المدرسة

تحدث إلى الطلاب عن الإعلانات وحثهم على التفكير فيما تحاول الشركات بيعه، فمن الجيد أن تركز على الإعلانات التي يراها الطالب بصورة متكررة، فيمكنك على سبيل المثال أن تجعل الطلاب يفكرون ويشككون في إدعاءات المعلنين عن طريق مطالبتهم بالتفكير فيما يتم الإعلان عنه. ما المنتج في هذا الإعلان؟ وفيما يستخدم؟ ولمَن يصلح؟ اسأل الطلاب عن الاستراتيجيات المستخدمة لبيع المنتج المعين. إذ يمكن أن يساعد ذلك الطلاب في التعرف على دور الإعلان في جعل المنتج يبدو جيدًا. فيما يلي بعض الأسئلة تساعد الطالب في بدء التفكير:

- ✓ هل يستخدم الإعلان المشاهير أو نجوم الرياضة للترويج للمنتج؟
- ✓ هل يربط الإعلان بين فكرة ومنتج - هل يجعل الإعلان الطالب أكثر نضجًا عند استخدام المنتج؟
- ✓ هل يروج الإعلان للمنتج بمنحك شيئًا مجانيًا- هل تحصل على لعبة عند شرائك وجبة أطفال من سلسلة وجبات سريعة؟

سيساعد هذا في توضيح النقطة التي تقول: لا يمكنك تصديق كل ما تراه على شاشة التليفزيون أو عبر الإنترنت أو غيرها من الوسائط -خاصة ما تراه في الإعلانات.

الأعمار من 12-13 سنة :

يفهم الطلاب في هذا العمر عادة الغرض من الإعلانات ويمكنهم استخدام المعلومات المعلنة لتحديد ما يريدون.

- . قد لا يفهمون كيف يجعل الإعلان الأشياء أغلى ثمنًا.
- . قد لا يتعرفون على الاستراتيجيات الخادعة لترويج المنتجات.

الأعمار أكبر من 14 سنة :

يفهم الطلاب كيفية عمل السوق ويمكن أن يكونوا متشككين بشأن إدعاءات المعلنين. يمكنك الحد من تأثير الإعلانات على الطلاب من خلال التحدث عن الطريقة التي تنتهجها الإعلانات لبيع الأفكار وكذلك المنتجات، فعلى سبيل المثال، تربط بعض الإعلانات بين المنتج والحياة "المثالية" التي يتمتع بها الأشخاص في الإعلانات. يبدأ الطلاب الأكبر سنًا في التفكير في التأثيرات الدقيقة للإعلان، فعلى سبيل المثال، يمكنك تشجيع الطلاب على التفكير في كيفية تأثير الإعلان على الأفكار المتعلقة بما يجب أن تبدو عليه هيئة الفتيات والفتيان والنساء والرجال وتصرفاتهم وما يأكلونه ويشربونه.

فيما يلي بعض الأسئلة لحث الطلاب الأكبر سنًا على التفكير:

- ✓ ما مدى حقيقة أسلوب الحياة المعلن عنه؟ هل تعرف أحدًا يعيش بهذه الطريقة؟
- ✓ هل الأطعمة والمشروبات المعلن عنها اختيارات صحية؟ لما لا يتم الإعلان عن الخضروات والفواكه مثل البرجر؟
- ✓ ماذا تقول الإعلانات عن الجنس والأسر وشكل الجسم والتنوع الثقافي؟ هل تعكس الإعلانات الحياة الحقيقية؟

3-4 المواقع والصور ومقاطع الفيديو غير اللائقة

1-3-4 فهم المواقع والمحتوى غير اللائق

هناك العديد من التقارير الحديثة التي تشمل وصول الطلاب المتعمد أو غير المتعمد للمواقع الإباحية والمشاعر والتصرفات التي يمكن أن تثيرها تلك المشاهد، ويمكن تعريف ذلك على إنه صور وأفلام لأشخاص لديهم علاقات غير لائقة أو يتصرفون بشكل سيئ عبر الإنترنت، ويشمل ذلك صورًا لأشخاص عراة وشبه عراة وأفلام للعرض أو التحميل من الإنترنت. وقد يشمل ذلك أيضًا صورًا غير لائقة شاركها شخص ما من الهاتف المحمول أو الكمبيوتر. وبعبارة أخرى، فإن المواد الإباحية هي مواد جنسية صريحة تهدف إلى إثارة الأشخاص الذين ينظرون إليها، وهي تشمل صورًا لأشخاص عراة أو شبه عراة يمارسون الجنس أو يبدون وكأنهم يمارسون الجنس أو يمارسون أنشطة جنسية.

2-3-4 كيف يتعرف الطلاب على المواقع والمحتويات غير اللائقة

عادة ما يري الأطفال من سن الروضة حتى الصف السادس الصور أو مقاطع الفيديو غير المناسبة بصورة عرضية، وقد يكون ذلك غير مريح ومزعج ومربك لأنهم يرون أشياءً لا يفهمونها، وقد يؤثر ذلك على مواقف الطلاب تجاه العلاقات الزوجية. ويمكن أن ترسل الكثير من الصور أو مقاطع الفيديو غير المناسبة والتي يمكن الوصول إليها بسهولة رسائل خاطئة مثل:

- ✓ لا توجد أهمية للموافقة المتبادلة والعلاقات الآمنة
- ✓ العلاقات العنيفة تبدو طبيعية وجذابة
- ✓ علاقات الحب ليست مهمة
- ✓ السلوك العدواني تجاه المرأة أمر طبيعي ومقبول

توجد اختلافات بين الجنسين فيما يخص التعرض والتصرف مع الصور أو مقاطع الفيديو غير المناسبة. يمكن أن تؤثر رؤية هذا النوع من الصور ومقاطع الفيديو على توجهات الطالب الجنسية وتوقعاته ومعتقداته. فقد ينظر الأولاد إلى هذا النوع من الصور بطريق إيجابية، مدعين بأنها أداة تعليمية، بينما تعتبرها الفتيات غير مرغوب فيها ومؤذية اجتماعيًا. تم ربط المواد الإباحية بـ:

- ✓ تصرفات غير واقعية في العلاقات بين الأزواج
- ✓ مواقف غير متكيفة بشأن العلاقات
- ✓ مزيد من المواقف المباحة جنسيًا
- ✓ المزيد من القبول للجنس العرضي
- ✓ المعتقدات بأن النساء كائنات جنسية
- ✓ المزيد من الأفكار حول الجنس
- ✓ عدم اليقين الجنسي

3-3-4 أين يرى الطلاب المواقع والمحتويات غير اللائقة؟

غالبًا ما يرى الطلاب المواقع الإباحية عبر الإنترنت، فهناك العديد من الصور ومقاطع الفيديو غير اللائقة على الإنترنت، كما أن اتصالات الإنترنت السريعة وتوفر الهواتف الذكية يؤدي إلى سهولة الوصول إليها. ولكن يرى معظم الطلاب صغار السن هذه الصور عن طريق الصدفة، فهم على سبيل المثال، قد:

- ✓ ينقرون على أشرطة جانبية أو إعلانات منبثقة على موقع ويب خاص بالألعاب - والتي يمكن أن تحتوي على مواد إعلانية تتضمن صورًا جنسية وروابط لمحتوى أكثر إثارة.
- ✓ يبحثون عن معلومات على الإنترنت ويحصلون على صور ذات محتوى جنسي عن طريق الصدفة
- ✓ يرون صورًا أو مقاطع فيديو غير لائقة عندما يعرضها الأصدقاء
- ✓ يرون أفعال جنسية متصنعة أو محتوى عنيف في برامج التليفزيون مثل Game of Thrones أو ألعاب فيديو مثل Grand Theft Auto.

4-3-4 مخاطر وأضرار المواقع غير اللائقة

إضافة إلى تأثير مشاهدة المواقع الإباحية على السلوك الجنسي للطالب والمخاطر المرتبطة بذلك، فهناك أيضًا دليل يثبت أن مشاهدة الكثير من هذه المواد الإباحية قد يترافق مع السلوك المنحرف والقهري.

يجب أن يدرك المعلمون أن المواد الإباحية على الإنترنت يمكن أن يعثر عليها الطالب عن طريق الصدفة من خلال:

1- **الإعلانات المنبثقة العشوائية:** قد تظهر تلك العناصر إذا قام الطالب بتنزيل برنامج مجاني
2- **محتوى تم مشاركته على وسائل التواصل الاجتماعي:** البث المباشر أو مواقع ويب تقدم محتوى مجاني
3- **البحث الحثيث عن محتوى صريح عبر الإنترنت:** يبحث الطلاب بدافع الفضول أو ربما لأن الأصدقاء يتحدثون عن الأمر.
4- **التعرض العرضي:** قد يقوم الطلاب بطريق الخطأ بكتابة كلمة أو عبارة خاطئة في محرك البحث على الإنترنت أو النقر عن طريق الخطأ على رابط يؤدي إلى شيء يبدو إنه مثير ولكن يتضح أنه إباحي.

على الرغم من توفر المواد الإباحية عبر الإنترنت، إلا أنه بموجب الخطط الجديدة، سيتم استقبال المستخدمين بصفحة تحذيرية تطلب منهم تسجيل الدخول عبر نظام التحقق من العمر، وسيطالب المستخدمون بتقديم إثبات شخصية في شكل بطاقة ائتمان أو رخصة قيادة قبل وصولهم إلى محتوى خاص بالبالغين. وقد يرى المستخدمون أيضًا صورًا ومواقع فيديو غير لائقة على مواقع ألعاب الأطفال المجانية، حيث أُختطفت بعض الشخصيات الكارتونية المحببة لدى الأطفال لتؤدي تمثيلات إباحية - وهو ما يؤلم الأطفال كثيرًا. لذا، يجب أن يكون الآباء على دراية بالصور ومقاطع الفيديو غير المناسبة على الإنترنت. هناك بعض الإرشادات للمساعدة إذا وجد الطلاب/الأطفال هذا النوع من الصور أو مقاطع الفيديو عبر الإنترنت. وقد تشير بعض أو كل العلامات التالية إلى مشاهدة طفلك لمواد إباحية:

1- علامات عن النشاط الجنسي السابق لأوانه أو الاهتمام المتزايد بالجنس واستخدام لغة جنسية.
2- رسوم غير مفهومة تُدفع من خلال بطاقة الوالد الائتمانية
3- يقوم الطالب بتبديل الشاشات بمجرد اقتراب أحد الوالدين من الجهاز الرقمي.
4- تبدأ النوافذ المنبثقة غير الملائمة والصريحة في الظهور على أجهزتك الرقمية.
5- تغير السلوك - ربما يصبح الطالب أكثر عدوانية أو يحيط أنشطته بالسرية.
6- قد يكشف سجل المتصفح عن مصطلحات البحث المستخدمة أو المواقع التي تم زيارتها والتي تشعر بأنها غير ملائمة.

هناك بعض العلامات التي يمكن للمعلمين إدراكها والتي تؤثر على الطلاب:

1- تشوش فهم الطلاب
2- تأثر نمو الطلاب تحديدًا
3- يمكن أن يظهر الطلاب علامات على سلوكهم الجنسي المبكر
4- قد يصاب الطلاب بمشاعر القلق أو الاكتئاب.

5-3-4 التحدث إلى الطلاب عن المواقع والمحتويات غير اللائقة

تحدث مع الطالب عن المواد الإباحية سرًا حسب عمره، فهذه تعد واحدة من أفضل الطرق لحمايته/لحمايتها من تأثير الإباحية. اذكر باختصار عند تناول كيفية توفير الأمان عبر الإنترنت كيفية ظهور المواد الإباحية، واقترح أن يتحدث الطالب إلى والديه عند الحاجة إلى طرح المزيد من الأسئلة.

ينبغي أن يكون المعلمين على دراية بما يلي:

1- يمكن للمحادثات المناسبة حسب العمر أن تساعد الطلاب على معالجة ما يصادفونه عبر الإنترنت وتعزيز أهمية العلاقات المحترمة.

2- أما بالنسبة للأطفال الصغار، فإن التحدث عن الصور أو مقاطع الفيديو غير المناسبة قد يجعلهم فضوليين أكثر عرضة لاستكشافها بأنفسهم. ولكن لا بأس من تأخير تلك المحادثة إذا كان الطلاب يتحدثون معك عن ما يشاهدونه عبر الإنترنت، وكنت متأكدًا من أنهم لم يروا محتوى إباحي.

3- **اشرح ماهية الإباحية بعبارات عامة** ولماذا يُفضل تجنبها. أخبرهم أن هذا النوع من الصور ومقاطع الفيديو ليست مناسبة للأطفال. يتطلع بعض البالغين لمشاهدة مثل تلك الصور، ولكنها ليست مناسبة للطلاب، إذ إنها تعرض أشياء لا يمكن للأطفال فهمها. يجب ألا ينظر الطلاب إلى مثل تلك الصور إذا رأوها صدفة عبر الإنترنت.

4- وإذا كان لدى الطالب أسئلة، فمن الأفضل أن تجيبه عنها باختصار وأمانة ودون الخوض في التفاصيل، وإذا لم تعرف إجابة أحد الأسئلة، فلا بأس أن تقول له أنك ستبحث في الأمر وتعود إليه. وعندما تتحدث إلى الطلاب عن تلك الصور ومقاطع الفيديو، فمن المهم أن تعرف ما يعرفه الطالب بالفعل وتوضيح أي لبس. وللقيام بذلك، يمكنك طرح بعض الأسئلة والتي تشمل على سبيل المثال:

- ✓ هل سمعت عن وجود صور لأناس عراة على الإنترنت؟
- ✓ وما الذي سمعته عن تلك الصور؟
- ✓ هل تحدث أي من زملائك عن مثل تلك الصور في المدرسة؟
- ✓ هل سبق لك أن صادفت أو عرض عليك صورًا لبالغين عراة؟
- ✓ هل لديك أي أسئلة حول الأشياء التي سمعتها؟

يمكن أن يبدأ الحديث حول المواد الإباحية عندما يكون الطلاب صغارًا في السن، ولكن هذا يعتمد على نضجهم ومدى قدرتهم على استخدام الإنترنت. المبدأ التوجيهي حول كيفية تحدث المعلمين عن الصور أو مقاطع الفيديو غير المناسبة بناءً على أعمار الطلاب:

الأعمار 5-12 سنة

1- **تجنب إعطاء "الكثير من المعلومات"** اجعل المناقشة مفتوحة، خاصة مع الطلاب الأصغر سنًا، مع الإجابة عن الأسئلة بأمانة وإيجاز، ثم اسأل "هل لديكم أسئلة أخرى؟" أو "هل هذا يفسر الأمر بما فيه الكفاية؟"

2- **حل المشكلات معًا:**

- ✓ اسأل الطلاب عن ما إذا كانوا يعتقدون أن البحث عن مثل تلك الأشياء عبر الإنترنت شيء جيد. (تلميح: ليست فكرة جيدة!)
- ✓ شجع الطلاب على التفكير في طرق للبقاء آمنين. نَوِّهْ إلى المشورة حول القواعد وسياسات التكنولوجيا.

3- **الاعتراف بضغوط الأقران:**

- ✓ إذا عُرض على الطلاب صور ومقاطع فيديو غير مناسبة من قبل أقرانهم أو طلاب أكبر سنًا، فتحدث عن أشياء مثل ضغط الأقران والقدرة على قول كلمة "لا" و تجنب الضغط الجماعي.
- ✓ أكد على حقيقة أن مشاركة الصور ومقاطع الفيديو غير المناسبة مع الأصدقاء ليست فكرة جيدة على الإطلاق.

الأعمار 13-18 سنة

1- **حاول أن تحافظ على الثقة:** تذكر عند التحدث إلى الطلاب أن محاولات التحكم في تفكيرهم أو سلوكهم قد تؤدي إلى ابتعادهم عنك ويصبح سلوكهم دفاعيًا.

2- **اشرح وافهم الفرق بين الإباحية والحياة الحقيقية:** لا تعد المواد الإباحية وسيلة جيدة لإمداد الطلاب بمعلومات عن الجنس، إذ يمكن أن تؤثر تلك المواد على شعورهم بذواتهم وتدمر العلاقات وتؤثر على العلاقات الإيجابية وتؤثر على صحتهم النفسية. وقد يصعب عليهم أيضًا فهم معنى كلمة "الرضا".

3- **تحدث عن الرضى والاحترام والأمان:**

- ✓ أخبر الطلاب أن عدم الاحترام والعنف وسوء المعاملة ليسوا أشياء جيدة وأنهم مسؤولون في النهاية عن سلامتهم واحترامهم من قبل الآخرين.
- ✓ ساعد المراهقين على إدراك أن ما يرونه في الصور ومقاطع الفيديو غير المناسبة غالبًا ما يكون غير حقيقي ومبالغ فيه ونادرًا ما يكون آمنًا.

4- **تحدث عن أهمية الألفة في العلاقات الوثيقة:** تقرب الألفة الناس من بعضهم البعض، بما في ذلك الروابط المألوفة والفريدة بين الأصدقاء والشركاء.

5- **ساعد الطلاب في فهم استجاباتهم:** يصل الشباب والشابات إلى محتويات غير لائقة بسبب الفضول وسهولة الوصول وقلة الخبرة. إذ يختبر أي طالب سن البلوغ، ويرى بعض الطلاب محتويات غير لائقة قبل أن يتمكنوا من فهمها عاطفيًا.

6- **حثّ الطالب على عدم مشاهدة المواد الإباحية:** ناقش الموضوع بعقل مفتوح وأجب عن الأسئلة بأمانة قدر المستطاع. حث الطلاب على عدم مشاهدة صور ومقاطع فيديو غير مناسبة، وإذا رأوا أي منها، فعليهم استشارة شخص بالغ.

6-3-4 **ماذا** يجب على المعلمين فعله **إذا اكتشفوا أن الطلاب يبحثون عن محتوى غير لائق عبر الإنترنت**

1- **ابق هادئًا:** حاول أن تعالج الموقف بهدوء. وإذا كنت منزعجًا أو غاضبًا، فقد يشعر الطالب أنه لن يأتي إليك في المستقبل ليطلعك على مخاوفه.

2- **استمع وقيّم وتوقف للحظات:**

- ✓ إذا قام الطالب بعرض محتوى صريح عن طريق الخطأ، فاطلب منه شرح التفاصيل حتى تتمكن من المساعدة في إدارة الموقف، فعليك أن تكتشف على سبيل المثال كيفية عثورهم على المحتوى وأين حدث ذلك ومن قام بعرضه عليه (إذا كان هناك شخص قام بذلك) وكيف شعر عند رؤية هذا المحتوى.
- ✓ قد يكون من المغري إعطاء محاضرة مركزة عن هذا الأمر، ولكن لا يكون هذا في بعض الأحيان هو الخيار الأفضل. خذ بعض الوقت لتضع نهجًا للموضوع. وسيكون لهذا الأمر نتيجة أفضل عندما يظل الجميع هادئين.

3- **طَمْأن الطالب أنه ليس في مأزق:**

- ✓ حاول أن تفهم بدلاً من أن تنتقد أو تعاقب.
- ✓ فعندما يخشى الطالب العقاب، قد ينغلق على نفسه، وقد يتردد في التحدث وقد يكافح من أجل الاستماع أو الفهم، وقد يؤدي ذلك إلى إخفاء الطالب سلوكه أو يتجنب الاقتراب منك في المستقبل.
- ✓ وإذا قال الطالب إنه لم يشاهد (أو عرض عليه) مواد إباحية ولكنك تعلم إنه لا يقول الحقيقة، فمن الأفضل أن تخبرهم بما تعرفه بدلاً من أن تغضب منهم بسبب الكذب. ومن المحتمل أن تكون المحادثة غير فعالة إذا كنت منزعجًا وكان الطالب مدافعا عن نفسه.

4- **كن حساسًا حيال شعورهم:**

- ✓ من المهم أن تتحدث إلى الطالب عن شعوره حيال المحتوى، فهذا يجعل المحادثة أقل مواجهة ويسمح له بالتحدث صراحة عن تجربته.
- ✓ هل يشعر الطالب بالرضا أو السوء أو الأمان أو الخوف أو عدم الراحة أو الفضول أو الاشمئزاز أو أي شيء آخر؟ يعد أي أو كل تلك المشاعر ردود فعل طبيعية.
- ✓ اطلب المساعدة الاحترافية إذا كنت تعتقد أن الطالب مستاء جدًا أو يكافح من أجل فهم ما شاهده.
- ✓ شجع الطالب على التحدث إليك حيال أي تساؤل يتعلق بما شاهده على الإنترنت، ودعه يعرف أن باستطاعته التحدث إليك في أي وقت.

4-4 المراسلة غير المناسبة والتحرش الجنسي

4-4-1 ما هي المراسلات الجنسية؟

المراسلات الجنسية هي الرسائل والصور الجنسية للشخص نفسه أو لأشخاص آخرين والتي يرسلها شخص ما أو يستقبلها أو يعيد إرسالها إلى شخص آخر، ويتم ذلك بين الهواتف المحمولة بصفة أساسية. ويمكن أن يتم ذلك أيضًا عن طريق استخدام جهاز كمبيوتر أو أي جهاز رقمي آخر وفي معظم الأحيان يتم مشاركة هذه الصور عن طريق النشر على الإنترنت ووسائل التواصل الاجتماعي الأخرى، ويمكن أن تخص تلك الصور ناشريها أو أشخاص آخرون عراة أو شبه عراة. وقد يصف الطالب هذا النوع من الرسائل بأنها مرسلات جنسية، وقد يستخدم مصطلحات أخرى مثل صور "عارية" أو "صورة شخصية مثيرة". ولا تزال مشاركة الطلاب وتأثيرهم في هذا النوع من التصرف أو إنشاء صور جنسية لأنفسهم بشكل مصدر قلق، فالمراسلات الجنسية ليست مشكلة بسيطة، ولكن يمكنك مساعدة الطلاب على فهم العواقب وكيف يمكن أن يشوه ذلك سمعتهم، حتى يتمكنوا من اتخاذ خيارات مسؤولة.

4-4-2 التحرش الجنسي عبر الإنترنت

تم الربط بين الطبيعة الجنسانية للمراسلات الجنسية والآثار النفسية والاجتماعية السلبية المحتملة للانخراط في النشاط وتجربة التحرش الجنسي عبر الإنترنت، خاصة بالنسبة للفتيات. ويتضمن هذا عددًا من السلوكيات المختلفة، بما في ذلك التحرش الجنساني، كالمشاركة غير الرضائية للصور الجنسية بغرض المضايقة أو الإحراج واستخدام لغة جنسية أو كتابة ألفاظ مسيئة في التعليقات والاهتمام الجنسي غير المرغوب فيه. وتم تصنيف التحرش الجنسي عبر الإنترنت إلى أربعة أنواع رئيسة. وغالبًا ما يتم اختبار تلك السلوكيات المختلفة في وقت واحد ويمكن أن تتداخل مع تجارب التحرش الجنسي التي تتم دون الاتصال بالإنترنت.

1- **المشاركة غير الرضائية لصور ومقاطع فيديو حميمة**: وتشمل مشاركة صور ومقاطع فيديو جنسية لأي شخص دون موافقته أو التقاطها دون موافقته.

2- **الاستغلال والإكراه والتهديد:** ويحدث ذلك عندما يتلقى شخص ما تهديدات جنسية أو يُكره على المشاركة في سلوك جنسي عبر الإنترنت أو يتم ابتزازه بمحتوى جنسي.

3- **التنمر الجنسي:** ويحدث ذلك عندما يتم استهداف شخص ما أو إقصاؤه بشكل منهجي من مجموعة أو مجتمع ما عن طريق استخدام محتوى جنسي مذل أو مزعج أو يتسم بالتمييز.

4- **الجنسنة غير المرغوب فيها:** يحدث ذلك عندما يتلقى شخص ما طلبات جنسية أو تعليقات أو محتوى غير مرغوب فيه.

4-4-3 ما يحتاج المعلمون معرفته عن "الاستدراج"

يشير الاستدراج إلى عملية اختلاط اجتماعي ينخرط خلالها أحد البالغين مع الطلاب أو المراهقين بغرض الاستغلال الجنسي عبر الإنترنت (قد تشمل تلك العملية جوانب خارج الإنترنت). هذا وقد أسفرت بعض الدراسات التي اكتشفت مدى انتشار "الإغراءات الجنسية" أو "الاستدراج" (أي قيام أحد البالغين بتشجيع طالب ما على الحديث أو القيام بشيء جنسي أو مشاركة معلومات جنسية شخصية)، وقد قدم الطلاب بشكل عام نتائج متنوعة اعتمادًا على خصائص عينة البحث والطريقة المستخدمة.

4-4-4 الاعتراف باستغلال الأطفال جنسيًا

يعد استغلال الطالب جنسيًا صورة من صور الإساءة الجنسية، ويحدث ذلك عندما يستفيد شخص ما أو مجموعة من عدم توازن القوة لإكراه طالب دون 18 عامًا أو التلاعب به أو خداعه لممارسة نشاط جنسي مقابل:

- ✓ شيء ما يحتاجه أو يرغب فيه
- ✓ ميزة مالية أو تعزيز مكانة مرتكب الجريمة أو الميسر لها
- ✓ قد يتم استغلال الضحية جنسيًا حتى لو بدا أن النشاط قد تم بالتراضي. ولا ينطوي استغلال الطالب جنسيًا على الاتصال الجسدي بصفة دائمة، إذ قد يحدث ذلك أيضًا عبر استخدام التكنولوجيا.

4-4-5 ما الذي يتمنى الطلاب أن يعرفه آباؤهم عن الرسائل غير الملائمة

قد يعتقد البالغون أن المراسلات الجنسية أمر محفوف بالمخاطر تم إكراه المراهقين على ممارسته، وعلى الرغم من وجود مخاطر متضمنة ويمكن الضغط على الطلاب لإرسال صور ومقاطع فيديو غير لائقة أو يصير الطالب متأرجحًا بسبب تأثير أقرانه عليه، إلا أن الأمر ليس بتلك البساطة. فغالبا ما يعتبر الطلاب المراسلات الجنسية أمرًا ممتعا ومرضيًا، وقد تعتبر طالبة ما وكذلك أصدقاؤها المراسلات الجنسية جزءًا من بناء العلاقات والثقة بالنفس واستكشاف الحياة الجنسية وأجسادهن وهوياتهن، ويقلق الطلاب بشأن مشاركة صورهم مع أشخاص آخرين بما في ذلك أصدقائهم وأفراد أسرهم، لذا،

يحاول الكثيرون تقليل تلك المخاطر من خلال أخذ صور لأشخاص يثقون بهم أو أشخاص هم على علاقة جادة بهم أو يأملون في ذلك، ومع ذلك يرسل بعض الطلاب صورًا إباحية لأشخاص لم يقابلوهم من قبل، لذا يجب أن يدرك الطلاب أن إرسال صورًا وفيديوهات غير لائقة هو أمر محفوف بالمخاطر، حيث يمكن إعادة إرسال صور تم مشاركتها لأشخاص آخرين دون موافقة أصحابها، فبمجرد إرسالك صورة لأحدهم تفقد التحكم بها، حيث يمكن مشاركتها مع أشخاص آخرين وفي جميع أنحاء وسائل التواصل الاجتماعي، ويمكن للمعلم أن يوضح أيضًا إنه بمجرد نشر الصور على الإنترنت يكون مسحها صعب جدًا، كما إنه من المهم أيضًا مساعدة الطلاب على فهم العواقب القانونية المترتبة على إرسال صور ومقاطع فيديو غير لائقة.



6-4-4 لماذا تشكل المراسلات غير اللائقة خطرًا على الطلاب

عند التقاط الصور الجنسية ومشاركتها دون موافقة صاحبها، تصبح المراسلات الجنسية مشكلة خطيرة، فإذا تم مشاركة صور أو فيديو إباحي لأحد الطلاب عبر الإنترنت، فقد تُنشر على مواقع التواصل الاجتماعي أو يتم إعادة إرسالها لأصدقاء وأشخاص لا يعرفهم الطالب على الإطلاق، وقد تصبح تلك الصور جزءًا من البصمة الرقمية للطالب وتظل باقية في المجال العام إلى الأبد، وكذلك إذا شاهد الناس صورًا جنسية لأحد الطلاب، فقد يشعر/تشعر بالحرج والذنب والخجل وعدم الراحة حيال القيام بأشياء عادية مثل الذهاب إلى المدرسة أو ممارسة الرياضة، وقد يكون الموقف مخز ويشعر الطالب بأن سمعته قد تضررت، وقد يتسبب الأمر أيضًا في إفساد علاقات الصداقة وعلاقات شبكات التواصل الاجتماعي. وقد يتعرض الطالب بسبب إرسال صور غير ملائمة للتنمر على الإنترنت، فعلى سبيل المثال عندما يشارك الناس صورًا لطالب فقد يعلقون عليها أيضًا بتعليقات مسيئة أو يهاجمون سمعته أو يلقبونه بألقاب مسيئة مطالبين بمزيد من الصور أو يطلبون أشياء أخرى غير ملائمة، وعادة ما تتعرض الفتيات لهذا النوع من التنمر والنقد بنسب تزيد عن الأولاد، ويُعزى ذلك إلى أن بعض الناس يطبقون معايير مختلفة بسبب الجنس، وقد يؤدي هذا الموقف أيضًا -في الحالات القصوى- إلى مشاكل نفسية مثل الاكتئاب أو الأفكار الانتحارية.

7-4-4 أهمية التحدث إلى الطلاب عن الرسائل غير اللائقة

يرغب الطلاب في أن يكونوا قادرين على التحدث بصراحة وصدق مع آبائهم بشأن المراسلات الجنسية، ويعد التحدث إلى الطلاب أحد أفضل الطرق لتعليمهم أمورًا حول الصور غير اللائقة وما يجب عليهم فعله إذا رأوا أيًّا منها، كما أنها طريقة جيدة تساعدهم على فهم مخاطر إرسال صور ومقاطع فيديو غير لائقة. فعندما يتحدث المعلمون والطلاب في نقاش مفتوح حول إرسال صور وفيديوهات غير لائقة، سيتمكن الطرفان من فهم المواقف التي قد تؤدي إلى مثل تلك الحوادث قبل وقوعها، كما أن معرفة الأشياء التي يجب تجنبها والأمور التي يجب القيام بها عند رؤية صورًا عارية قد يُساعد الطلاب على الشعور بارتياح أكبر إذا رغبوا في التحدث إلى شخص بالغ عند حدوث أمر ما، ولن يشعروا بالرهبة للكشف عن مواقف مثيرة للقلق.



8-4-4 كيفية التحدث عن الرسائل غير اللائقة

قد تشعر بالحرج حيال التحدث مع الطلاب حول إرسال صورًا وفيديوهات غير لائقة، ولكن إليك بعض الأسئلة التي يمكنك طرحها لبدء مناقشة:

- ✓ هل تعرف أحدًا من طلاب المدرسة أرسل أو استلم صورًا شخصية مثيرة أو صورًا غير لائقة؟ هل فعلوا ذلك بغرض المرح أو المغازلة؟
- ✓ هل أرادوا هم أنفسهم إرسال تلك الصور أم حثهم شخص آخر على فعل ذلك؟
- ✓ هل أرسلت صورًا عارية أو جنسية من قبل؟
- ✓ هل لديك مزيد من الأسئلة أو التعليقات حول تلك الموضوعات؟

عندما يكون لدى الطلاب أسئلة عن المراسلات الجنسية، حاول أن تجيب عن الأسئلة بأمانة وصراحة قدر الإمكان، وفي حالة كان هناك مخاوف بشأن إرسال صور أو مقاطع فيديو غير لائقة، فعليك أن تفسر مخاوفك للطلاب ولماذا يجب ألا يقوموا بإرسال رسائل جنسية، فالتواصل يمنح الطلاب فرصًا للانفتاح. ومن المرجح أن يكون لإرسال صور ومقاطع فيديو غير لائقة عواقب سلبية، وذلك عندما يتم الضغط على الشخص الذي أرسل تلك الرسائل للقيام بذلك. وفيما يلي بعض الإرشادات حول كيفية تحدث المعلمين عن المراسلات الجنسية:

1- **تحدث عن خصائص العلاقة الصحية:** اسأل الطلاب عما إذا كان من المناسب على الإطلاق أن يقوموا بمضايقة شركائهم أو إحراجهم أو عزلهم أو التحكم فيهم، واجعلهم يدركون أن تلك السلوكيات غير لائقة بأي حال من الأحوال.

2- **أعط معلومات ونماذج عن العادات العاطفية الصحية:** شجع الطلاب على عدم إرسال أو الرد على شيء ما في حالة الغضب، بل "الابتعاد" عن الموقف والانتظار حتى تهدأ الأمور.

3- **الحديث عن أدوار الجنسين:** اشرح كيف يشعر الفتيات والفتيان بأن عليهم التصرف بطريقة معينة بسبب الأدوار الجنسانية الراسخة.

4- **عند وجود الطالب في علاقة غير صحية:** كن واضحًا في أنك تعتقد أن تلك العلاقة غير صحية، لكن لا تحاول أن تحضهم على تركها، وبدلًا من ذلك، شجع الطالب أو الطالبة لقضاء وقت أطول مع العائلة والأصدقاء. وتحدث إلى أصدقاء الطالب لمعرفة ما إذا كان لديهم مخاوف مماثلة.

5- **ناقش الطرق المناسبة لإظهار اهتمامك بشخص ما:** حاول أن تتصل بالطالب وأظهر له/ لها مدى اهتمامك. وكن شفافًا واذهب بعيدًا بهدف المساعدة.

4-4-9 ماذا يجب عليك فعله إذا تلقي الطالب رسالة غير لائقة ماذا عليك فعله؟

في حالة تلقي الطالب رسالة جنسية صريحة غير مرغوب فيها، فتحدث عن كيفية الرد عليها:

- ✓ فإذا كان المرسل صديقًا لهذا الطالب، فاطلب منه حذف الرسالة وإخبار هذا الصديق بألا يرسل المزيد من الرسائل المشابهة، وشجعه على قول كلمة "لا" بطرق تشعره بالراحة.
- ✓ أخبر الطالب بعدم إعادة توجيه الرسالة.
- ✓ وفي حالة عدم معرفة الطالب لمرسل الرسالة، فأخبره بعدم الرد وحظر المرسل.
- ✓ اطلب من الطالب إخبارك أو أي شخص بالغ يثق فيه في حالة استمرار حصوله على صور غير مرغوب فيها.

وإذا كان الطالب يحصل على مواد جنسية من شخص غير معروف لديه وتعتقد إنه طالب في نفس المدرسة، فاتصل بالمدرسة.

وفي حالة الاعتقاد بأن الحادثة مسألة جنائية، خاصة إذا ثبت أن شخصًا بالغًا يتصل بالطالب، فقدم شكوى إلى الشرطة، فعلى سبيل المثال، يعد الأمر جريمة إذا ثبت أن شخصًا ما يرسل لطالب صورًا عارية غير مرغوب فيها.

4-4-10 عندما يرسل الطالب رسالة غير لائقة: ماذا عليك فعله؟

إذا أرسل الطالب رسالة جنسية صريحة ثم ندم على ذلك الفعل، فمن المهم دعم الطالب وطمأنته أنكما ستعالجان الأمر معًا:

1- اسأل الطالب عن سياق الرسالة، وهل شعر الطالب بالضغط عليه لإرسالها أم كان الأمر بالتراضي؟ وتحقق أيضًا من محتواها ولمن أرسلها

2- انصح الطالب بحذف الرسالة من هاتفه المحمول أو الكمبيوتر أو أي مكان تم تخزينها فيه.

3- شجع الطالب على مطالبة الشخص الذي تلقاها بحذفها.

4- إذا حمّل الطالب صورة لنفسه/نفسها على أحد مواقع التواصل الاجتماعي، فشجعه/شجعها على حذفها، وعرفه بكيفية حذف الصور أو كيفية التواصل مع الموقع لحذفها.

5- شجع الطالب على سؤال نفسه الأسئلة التالية بشأن ما شاركه:

- ✓ هل هذا ما أريد أن يعرفه الناس عني؟
- ✓ هل يستطيع أي شخص استخدام تلك المواد في إيذائي؟ هل سأشعر بالضيق إذا تم مشاركة تلك المواد مع أشخاص آخرين؟
- ✓ ما هو أسوأ شيء يمكن أن يحدث إذا شاركت هذه المواد؟

وإذا اعتقدت أن الحادثة مسألة جنائية، فقدم شكوى إلى الشرطة. فعلى سبيل المثال، تعد مطالبة شخص بالغ طالب ما بإرسال صور جنسية صريحة جريمة يعاقب عليها القانون.

11-4-4 عند قيام الطالب بمشاركة رسالة غير لائقة أرسلها شخص ما: ماذا عليك فعله؟

إذا شارك الطالب صورة جنسية صريحة لشخص آخر، فمن المهم دعم الطالب وطمأنته أنكما ستحلان المشكلة معًا:

1- اسأل الطالب عن سياق تلك الرسالة الجنسية ومن أرسل تلك الرسالة التي شاركها ولماذا قام بذلك؟ وتحقق أيضًا من محتواها ولمن أرسلها.

2- شجع الطالب على مطالبة الشخص أو الأشخاص الذين تلقوا الرسالة بحذفها، وساعده على القيام بذلك.

3- شجع الطفل/المراهق على طرح الأسئلة التالية عند مشاركة شخص ما صورًا ورسائل غير لائقة معهم:

- ✓ هل قصد الشخص الموجود في هذه الصورة مشاركتها؟
- ✓ هل حصل المرسل على إذن صاحب الصورة؟
- ✓ كيف سيكون شعوري إذا قام شخص ما بمشاركة شيء مشابه عن نفسه؟

4- إذا حمّل الطالب تلك الصورة على وسائل التواصل الاجتماعي أو على أي موقع آخر، فساعده في التواصل مع تلك المواقع لحذفها.

5- وإذا قام الطالب بإرسال مواد جنسية إلى شخص ما في المدرسة، فتحدث إلى المدرسة واطلب مساعدتها للتأكد من عدم مشاركة الصور.

6- ساعد الطالب على الاتصال بالشخص الذي أرسل الرسالة الجنسية لإخباره بمشاركتها.

7- طمئن الطالب بأن مشاركة الصورة ليس خطأ منه.

8- تحدث إلى المدرسة من أجل المساعدة في تحديد الأشخاص الذين قد يملكون الصور ويعرفون المواقع التي قد يتم مشاركة الصورة عليها. إذا تم تحميل الصور على وسائل التواصل الاجتماعي أو مواقع الويب الأخرى، فساعد الطالب على اكتشاف أماكن وجودها واتصل بهذه المواقع لطلب حذفها.

9- شجع الطالب على حظر أي شخص يكتب تعليقات عدوانية أو يسأل عن صور غير مرغوب فيها. وعرّف الطالب بكيفية حظر أي مرسل غير مرغوب فيه.

كما يعد من الأفكار الجيدة أن تشجع الطالب على أن يسأل نفسه الأسئلة التالية:

- ✓ هل قصد الشخص الموجود في هذه الصورة مشاركتها؟
- ✓ وفي حالة قيام شخص آخر بإرسال الصورة، فهل حصل على إذن الشخص الموجود فيها؟
- ✓ كيف سيكون شعور الطالب إذا قام شخص ما بمشاركة شيء مماثل معه/معها؟

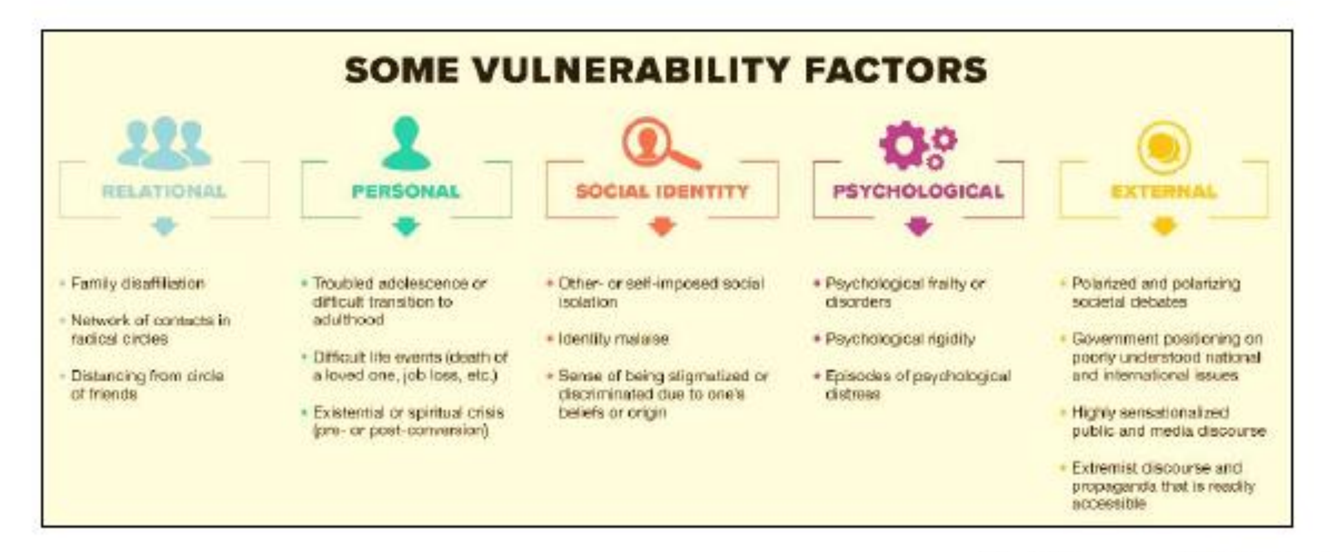
من المهم أن يدرك الطلاب أن مشاركة الصور الجنسية دون موافقة أصحابها يُعد نوعًا من التحرش أو الاعتداء الجنسي ويمكن أن يعرضهم للمساءلة القانونية. وفي حالة كانت المسألة جنائية، فقدم شكوى إلى الشرطة. على سبيل المثال، يُعد إجبار الطالب على مشاركة صورة أو أكثر جريمة وكذلك إذا ثبت تدخل أحد البالغين في الأمر.

4-4-12 أهمية العلاقات المحترمة

لا يعد إخبار الطالب بعدم إرسال صورًا لأناس عراة أو صور شخصية مثيرة أفضل طريقة لحمايته، وبدلًا من ذلك، تحدث إليه عن العلاقات المحترمة والمخاطر الجنسية والثقة. واشرح للطلاب أن إرسال مثل تلك الصور والمقاطع غير اللائقة يُعد نشاطًا جنسيًا فعليًا، كما أن كل الأفعال الجنسية - بما في ذلك إرسال الصور ومقاطع الفيديو غير اللائقة - يتطلب موافقة الشريك، وأن خرق شرط الموافقة بمشاركة رسائل جنسية ليس سلوكًا محترمًا، كما إنه من غير المقبول مشاركة مواد جنسية تخص أشخاص آخرين أو إرسال صور عارية لشخص لم يطلبها. فعلى سبيل المثال، قد تقول "يجب أن تتأكد دائمًا من أن الشخص الآخر يرغب في التقاط صورًا عارية له قبل التقاطها، ولن يكون من المقبول أن تضغط على شخص ما لإرسال صورة فاضحة أو تجعله يشعر بالسوء لرفضه إرسال واحدة". كما من المهم أن يعرف الطالب أنه يملك الحق في أن يقول "لا"، وإنه ليس من المقبول أن يضغط شخصًا ما على الطالب بهدف فعل أي شيء جنسي، بما في ذلك إرسال صورًا جنسية لنفسه. ومن الجيد أيضًا أن يتدرب الطالب على قول كلمة "لا"، كما يمكنه أن يستخدم روح الفكاهة بقول "نعم، لما لا؟" ثم يرسل صورة لحيوان أو شخص ماسكًا عصا. أو يمكن أن يكتفي بقول "لا، أنا لا أرسل صور فاضحة لأنني لا أريد أن أخاطر برؤية الآخرين لها".

4-4-13 المراسلات غير اللائقة والقانون

بموجب القانون، تعد المراسلات الجنسية المتضمنة طلاب دون سن 18 عامًا جريمة جنائية حتى إذا تم ذلك بالتراضي، وبمقتضى بند الجرائم، يمكن النظر إلى هذا الفعل بوصفه صور إباحية لطالب أو فعل غير محتشم، وعليه يمكن إلقاء القبض على الطالب وإدراجه في سجل مرتكبي الجرائم الجنسية. وإذا تورط طالب في إرسال صور ومقاطع فيديو غير لائقة وقام شخص ما بإبلاغ الشرطة، فيمكن اتهام الطالب بحيازة مواد إباحية أو توزيعها على الطلاب، وفي هذه الحالة تقرر الشرطة ما إذا كانت ستوجه اتهامًا للشخص أم ستحاكمه اعتمادًا على خطورة الموقف. أما إذا تضمنت الرسائل الجنسية مضايقات أو تهديدات، فمن المرجح أن توجه الشرطة اتهامات. فعلى سبيل المثال، إذا استمر شخص ما في مضايقة الطالب عن طريق مطالبته بصور عارية أو استمر في إرسال صورة عارية له وهو لا يرغب فيها.



4-5 التطرف عبر الإنترنت

4-5-1 ما الذي ينبغي على المعلمين معرفته عن التطرف

يُعرف التطرف بأنه عملية تشمل اعتناق الفرد لقيم وآراء معينة حول موضوع ما ثم يصبح تدريجيًا أكثر تطرفًا ومن ثم يبدأ في الانحراف بعيدًا عن الآراء الطبيعية، كما يجد صعوبة بالغة في قبول الآراء المضادة. ويمكن أن تستند آرائه إلى موضوعات مختلفة مثل السياسية والدين والفلسفة من بين مواضيع أخرى، كما يمكن أن يؤدي التطرف في الحالات القصوى إلى العنف الإيديولوجي والذي يشمل الإرهاب. فهناك العديد من العوامل التي تؤثر على تطور المعتقدات الأيديولوجية لدى البعض وهناك أدلة تشير إلى أن الإنترنت يلعب دورًا كبيرًا في تسهيل مثل تلك العمليات بين الطلاب.

4-5-2 دور الإنترنت ووسائل التواصل الاجتماعي في نشر التطرف

كما هو واضح في هذا التقرير، يملك طلاب اليوم وصولاً عالميًا إلى الإنترنت من خلال أجهزة متعددة، وتعد شبكات التواصل الاجتماعي إحدى أهم الوسائط المفضلة لدى أغلب الطلاب، وهذه حقيقة تستغلها بعض الجماعات المتطرفة مما يجعل الطالب عرضة للإيذاء والدعاية من بعض هذه الجماعات الإسلامية اليمينية المتطرفة، كما يسهل الإنترنت عملية نقل المعرفة ونشر المعلومات على جمهور أكبر، وهو ما يساعد على تمدد التطرف الذاتي (حيث لا يتم أي تواصل مع إرهابيين أو متطرفين آخرين، سواء أكان ذلك شخصيًا أو افتراضيًا).

وإليكم فيما يلي خمس نتائج رئيسية:

1- يخلق الإنترنت المزيد من الفرص كي يصبح الشخص متطرفًا

2- يعمل الإنترنت كـ"غرفة صدى" وهو مكان يجد فيه الأفراد من يدعمون أفكارهم من ذوي التفكير المماثل.

3- تسريع عملية التطرف

4- السماح بحدوث التطرف دون تواصل جسدي

5- ازدياد فرص التطرف الذاتي

4-5-3 خصائص الطلاب سريعي التأثر والمجندين لهم

يكون المجندين بارعين للغاية في استهداف جمهور الشباب (مثل إتاحة ألعاب فيديو عبر الإنترنت بهدف الترويج للتطرف)، إذ تحول العديد من الطلاب سريعي التأثر إلى التطرف بعد أن شعروا بنبذ المجتمع لهم ووجدوا ضالتهم في شبكات التواصل الافتراضية عبر الإنترنت. وتشير التقارير إلى أن المؤشرات العامة لسرعة تأثر الطلاب هي على النحو التالي:

- ✓ التوتر الأسري
- ✓ الإحساس بالعزلة
- ✓ الهجرة
- ✓ البعد عن التراث الثقافي
- ✓ اختبار العنصرية أو التمييز
- ✓ الشعور بالفشل

4-5-4 مساعدة الطلاب الذين استدرجوا إلى آفة التطرف

يوفر موقع Prevent Duty إرشادات للمدارس ومقدمي الرعاية الطلابية حول منع انزلاق الطلاب إلى الإرهاب، كما تمثل القنوات جزءً رئيسًا في إستراتيجية الوقاية، فهي تدعم الأفراد المحفوفين بمخاطر الوقوع في براثن الإرهاب، حيث يستخدم المبرمجون نهج الوكالات المتعدد لحماية المجموعات سريعة التأثر عن طريق:

- ✓ تعريف الأفراد المحفوفين بالمخاطر
- ✓ تقييم طبيعة تلك المخاطر ومدى خطورتها
- ✓ تقديم أفضل خطة دعم للأفراد المعنيين

وإليكم هنا بعض الإرشادات التي تساعد في إثارة الموضوع ومنع تعرض الطلاب لأفكار متطرفة عن غير قصد:

1- كن ودودًا: دع الطلاب يعرفون إنك ستكون متاحًا لمساعدتهم في حالة تورطهم في مشكلات عبر الإنترنت - كما أنهم يستطيعون التواصل معك في حالة وجود مخاوف لديهم.

2- كن هادئًا وليس غاضبًا: من المرجح أن يكون الطلاب أكثر انفتاحًا وصراحة عندما يبقى الكبار هادئين حيال مواقف ما.

3- أخبر شخصًا ما: تأكد من أن الطلاب على دراية إنه في حالة وجود ما يقلقهم أو إذا كانوا غير مرتاحين للدخول إلى الإنترنت، فسيكون أفضل خيار متاح لديهم هو التحدث إلى أحد البالغين الذين يثقون به.

4- تحدث إليهم حول صداقاتهم عبر الإنترنت: حاول أن تكتشف مواقع الويب التي يصلون إليها، وأماكن التقائهم بأصدقاء الإنترنت وكيف يتواصلون مع بعضهم البعض وما هي المعلومات التي يشاركونها. وتحدث إليهم عن أهمية توخي الحذر حيال ما يشاركونه مع الآخرين عبر الإنترنت. وذكرهم بأن ليس كل من يقابلونه عبر الإنترنت يعد صديقًا إذ قد يكون لديهم دوافع خفية لإقامة علاقات صداقة معهم.

1- **لا تكن عدوانيًا:** تعد اعتقادات الطلاب وآرائهم موضوعًا حساسًا، لذا يتطلب الأمر حسن المعاملة، الأمر الذي يتطلب منك عدم استبعادهم أو إسكاتهم.

2- **كن آمنًا في الحياة الحقيقية:** عرّف الطلاب بأهمية تجنب لقاء شخص لا يعرفونه إلا من خلال الإنترنت دون حضور أحد الأبوين.

3- **شجعهم على مشاركة أفكارهم وآرائهم:** إذ لا يدرك العديد من الشباب الصغار حقيقة وعواقب الأفكار المتطرفة التي يعتنقونها والحجج التي ضدهم.

6-4 تعريف قابلية التأثر وجعل الشخص ضحية

يشير مصطلح قابلية التأثر إلى أن الشخص يتمتع بصفة أو خصائص تجعله عرضة للهجوم أو الإيذاء إما جسديًا أو عاطفيًا، كما يتحول الشخص إلى ضحية نتيجة لقيام شخص آخر بخداعه أو بسبب جهله، فالطفل البريء يكون عرضة للخطر على الإنترنت، فهو غالبًا ما يصدق ما يقوله الغرباء له.

4-6-1 من هي الفئات سريعة التأثر عبر الإنترنت؟

يبدو أن بعض الطلاب يكونون أكثر عرضة لمخاطر الإنترنت، فهم إما أن يكونون أكثر عرضة لمواجهة المخاطر أو عندما يواجهون خطرًا، فمن المرجح أن يجدوه ضارًا، أو أنهم يتميزون باختصار بأنهم أقل مرونة أو أقل قدرة على التكيف. وقد فحصت بعض الأبحاث تجاربهم عبر الإنترنت بمزيد من التفصيل:

1- الطلاب الذين يعانون من صعوبات عائلية: قد يعاني الطلاب الذين تربو في عائلة/ بيئات فوضوية من مشاكل جسدية أو نفسية و/ أو اعتداءات جنسية وإهمال، وقد يكونوا قد تعرضوا أيضًا لعنف منزلي و/أو انهيار الأسرة أو نشأوا في بيئة يتوفر فيها تعاطي المخدرات أو تناول الكحول، وقد يكون الطالب قد تلقى معاملة سيئة من الأم أو الأب أو ربما عانى من إيذاء أو إساءة ذات أثر عميق أو ربما التحق بنظام رعاية.

2- الطلاب ذوي الإعاقات: قد يعاني هؤلاء الطلاب من اعتلال جسدي مزمن أو لديهم إعاقات جسدية أو تعليمية أو احتياجات تعليمية خاصة.

3- الطلاب الذين يواجهون صعوبات سلوكية/عاطفية: قد يتعرض هؤلاء الطلاب لأعراض مختلفة مثل الميل إلى إيذاء النفس أو محاولة الانتحار أو تم تشخيص إصابتهم بحالة عقلية أو سلوكية.

4- الطلاب الذين يعانون من استبعاد الوصول - يختبر هؤلاء الطلاب إهمال النظام لهم، ويتمثل ذلك في عدم قدرتهم على الوصول إلى الخدمات المتاحة عالميًا للطلاب الآخرين.

4-6-2 ما ينبغي على المعلمين فعله لمنع تحول الطلاب إلى ضحايا للرسائل المزعجة والتصيد

1- **الرسائل المزعجة:** هذه هو المكافئ الالكتروني لرسائل البريد الإلكتروني غير الهامة، ويشير المصطلح إلى رسائل البريد الإلكتروني الكثيرة غير المرغوب فيها عادة. ولتقليل من تأثر الطلاب برسائل البريد الإلكتروني المزعجة، عليك بما يلي:

- ✓ تمكين الفلاتر في برامج بريدك الإلكتروني: يعرض معظم مقدمي خدمات الإنترنت (ISPs) وموفري خدمة البريد الإلكتروني مرشحات للرسائل المزعجة، وبالرغم من ذلك، ووفقًا لمستوى الضبط، قد ينتهي المطاف بالمستخدمين إلى حظر رسائل البريد الإلكتروني المرغوب فيها، كما يعد مراجعة مجلد الرسائل غير المرغوب فيه من آن لآخر فكرة جيدة للتأكد من عمل المرشحات بصورة مناسبة.
- ✓ الإبلاغ عن رسائل البريد الإلكتروني المزعجة: يساعد الإبلاغ عن الرسائل المزعجة أيضًا في منع وصول الرسائل إلى صندوق الوارد الخاص بك مباشرةً.
- ✓ **امتلك حضورك على شبكة الإنترنت:** احرص على إخفاء عنوان البريد الإلكتروني الخاص بك من ملفات التعريف على الإنترنت ومواقع التواصل الاجتماعي أو اسمح لأشخاص معينين فقط برؤية معلوماتك الشخصية.

2- **التصيد:** يهاجم المتصيدون الضحايا من خلال رسائل البريد الإلكتروني أو مواقع الويب الخبيثة (بالنقر على رابط) بهدف جمع معلومات شخصية ومالية أو إصابة جهازك بالبرامج الضارة والفيروسات.

3- **التصيد الموجه:**

- ✓ ينطوي التصيد الموجه على هجمات متخصصة للغاية ضد أهداف محددة أو مجموعات صغيرة من الأهداف بهدف جمع المعلومات أو التمكن من الوصول إلى الأنظمة.
- ✓ ويمكن أن يستخدم مجرمو الإنترنت العديد من التقنيات الخبيثة للهندسة الاجتماعية مثل الإشارة إلى وجود تحديث فني مهم أو عرض سعر منخفض لإغراء الناس.

4- **رسائل البريد الإلكتروني المزعجة والتصيد عبر شبكات التواصل الاجتماعي:** لا يقتصر ضرر الرسائل المزعجة والتصيد على رسائل البريد الإلكتروني فقط، فهي توجد بكثرة أيضًا على مواقع التواصل الاجتماعي. ويتم تطبيق نفس القواعد على مواقع التواصل الاجتماعي - فعندما يراودك الشك في أمر ما، قم بحذفه على الفور، كما ينطبق هذا الأمر على روابط الإعلانات وتحديثات الحالة والتغريدات والمشاركات الأخرى.

كن حذرًا من الأمور التالية حتى لا تكون ضحية:

- ✓ لا تبح بالمعلومات الشخصية أو المالية في أحد رسائل البريد الإلكتروني ولا ترد على إغراءات العروض الهادفة إلى طلب هذه المعلومات، ويتضمن ذلك الروابط التالية المرسلة في أحد رسائل البريد الإلكتروني.
- ✓ قبل إرسال معلومات حساسة أو إدخالها على الإنترنت، قم بفحص أمان لموقع الويب.
- ✓ انتبه إلى عنوان URL الخاص بموقع الويب. قد تبدو مواقع الويب الضارة متطابقة مع المواقع المشروعة، ولكنها قد تستخدم عنوان URL بهجاء أو مجال مختلف (مثل com مقابل net).
- ✓ إذا لم تكن متأكدًا ما إذا كان طلب البريد الإلكتروني مشروعًا، فحاول التحقق منه عن طريق الاتصال بالشركة مباشرة. اتصل بالشركة باستخدام المعلومات المقدمة في كشف الحساب، وليس المعلومات المقدمة في رسالة بريد إلكتروني.
- ✓ حافظ على نظافة الجهاز حافظ على تحديث جميع البرامج على الأجهزة المتصلة بالإنترنت - بما في ذلك أجهزة الكمبيوتر والهواتف الذكية والأجهزة اللوحية - لتقليل خطر الإصابة بالبرمجيات الضارة.

ماذا تفعل إذا كنت ضحية؟

- ✓ أبلغ الأشخاص المناسبين في المؤسسة، بما في ذلك مسؤولو شبكة الإنترنت، إذ يمكن أن يكونوا منتبهين لأي نشاط مشبوه أو غير عادي.
- ✓ راقب أي رسوم غير مصرح بها أضيفت لحسابك.

احم نفسك بهذا الإجراء: توقف، فكر ثم اتصل

- ✓ **عندما تكون في شك من أمر ما، قم بحذفه على الفور:** يحاول مجرموا الإنترنت اختراق معلوماتك الشخصية من خلال روابط البريد الإلكتروني والتغريدات والمنشورات والإعلانات، وإذا شعرت بالشك حتى وإن كنت تعرف المصدر فمن الأفضل حذفه أو قم بوضع علامة غير مرغوب فيه إذا كان ذلك مناسبًا.
- ✓ **فكر قبل أن تفعل شيئًا:** كن حذرًا من الاتصالات التي تطلب منك أن تتصرف فورًا، أو تقدم شيئًا يبدو جيدًا لدرجة يصعب تصديقها أو يطلب معلومات شخصية.
- ✓ **اجعل كلمة المرور جملة:** ويجب ألا تقل كلمة المرور عن 12 حرف كي تكون قوية، وركز على جمل أو عبارات إيجابية تحب التفكير فيها ويسهل تذكرها (على سبيل المثال "أنا أحب موسيقى الريف")، كما يمكنك استخدام المسافات في الكثير من المواقع!
- ✓ **حساب فريد من نوعه وكلمة مرور فريدة من نوعها:** يؤدي امتلاك جمل مرور منفصلة لكل حساب إلى عدم تمكن مجرمي الإنترنت من اختراق حساباتك، كما ينبغي الفصل بين حسابات العمل والحسابات الشخصية والتأكيد على أن حساباتك المهمة لها أقوى جمل مرور.
- ✓ **احرص على قفل تسجيل الدخول الخاص بك:** قم بتدعيم حساباتك عبر الإنترنت من خلال تمكين أقوى أدوات المصادقة المتاحة، مثل القياسات الحيوية أو مفاتيح الأمان أو رمز فريد لمرة واحدة من خلال تطبيق على جهازك المحمول. لا تكون أسماء المستخدمين وجمل المرور الخاصة بك كافية لحماية الحسابات الرئيسية مثل البريد الإلكتروني والخدمات المصرفية ووسائل التواصل الاجتماعي.

3-6-4 يجب ألا يغامر الطلاب عبر الإنترنت دون اتخاذ احتياطات أساسية

1- **الفيروسات:** الفيروسات هي برامج ضارة يمكن أن تنتقل إلى أجهزة الكمبيوتر والأجهزة المتصلة الأخرى بعدة طرق. وعلى الرغم من اختلاف الفيروسات بطرق عديدة، فقد صممت جميعها للانتشار من جهاز لآخر ونشر الخراب. ويعتقد في أغلب الأحيان أن الفيروسات مصممة لمنح المجرمين الذين يقومون بإنشائهم نوعًا من الوصول إلى الأجهزة المصابة.

2- **برامج التجسس:** تنطبق مصطلحات "برامج التجسس" و"البرامج الإعلانية" على العديد من التقنيات المختلفة، لكن يوجد شيئان يجب معرفتهما عنها، وهي:

- ✓ تتمكن تلك البرامج من تنزيل نفسها على الجهاز دون إذنك؛ وعادةً ما يتم ذلك عندما يزور المستخدم موقع غير آمن أو عبر مرفق.
- ✓ تتمكن تلك البرامج من جعل جهاز الكمبيوتر الخاص بك يقوم بأشياء لا ترغب في القيام بها، مثل فتح إعلان لا ترغب في رؤيته. تتمكن برامج التجسس في أسوأ الحالات من تتبع تحركاتك عبر الإنترنت وسرقة عبارات المرور و/أو تسوية الحسابات.

3- **شبكات البوتنت:** تشير إلى شبكات من أجهزة كمبيوتر مصابة ببرمجيات ضارة، مثل فيروسات الكمبيوتر والمسجلات الرئيسية والبرامج الضارة الأخرى. حيث يتم عادةً التحكم فيها عن بُعد بواسطة مجرمين بهدف كسب المال أو بدء هجوم على مواقع الويب أو الشبكات.

- ✓ وإذا كان جهاز الكمبيوتر مصابًا بهذه البرامج الضارة وجزءًا من البوتنيت، فإنه يتواصل ويتلقى تعليمات حول ما يفترض أن يفعله من أجهزة كمبيوتر "الأوامر والتحكم" الموجودة في أي مكان في جميع أنحاء العالم. يعتمد ما يقوم به جهاز الكمبيوتر الخاص بك على ما يحاول مجرمو الإنترنت تحقيقه.
- ✓ وتم تصميم العديد من شبكات البوتنيت لحصد البيانات، مثل عبارات المرور وأرقام الضمان الاجتماعي وأرقام بطاقات الائتمان والعناوين وأرقام الهاتف وغيرها من المعلومات الشخصية. ثم يتم استخدام البيانات لأغراض ضارة، مثل سرقة الهوية وتزييف بطاقة الائتمان وإرسال رسائل غير مرغوب فيها (إرسال رسائل بريد إلكتروني غير هامة)، وهجمات مواقع الويب وتوزيع البرامج الضارة.

4- **فيروس الفدية:** هذا نوع من البرامج الضارة التي تفتح ملفات الضحية وتغلقهم وتشفرهم ثم تطالب الضحية بدفع فدية لإعادتهم لها، ويستخدم مجرمو الإنترنت هذه الهجمات لمحاولة دفع المستخدمين للنقر على المرفقات أو الروابط التي تبدو مشروعة لكنها تحوي أكواد خبيثة. ويشبه فيروس الفدية "الاختطاف الرقمي" لبيانات قيمة - من الصور الشخصية والذكريات إلى معلومات العميل والسجلات المالية والملكية الفكرية. وقد يكون أي فرد أو مؤسسة هدفًا محتملًا لفيروس الفدية.

كيف يتعرف المعلمون على إصابة أجهزة الطلاب ببرامج ضارة:

- ✓ تلاحظ بطئ النظام أو تعطله أو عرض رسائل خطأ متكررة
- ✓ عدم قدرته على الغلق أو إعادة التشغيل
- ✓ يقدم مجموعة من النوافذ المنبثقة
- ✓ يقدم إعلانات غير لائقة أو إعلانات تتداخل مع محتوى الصفحة
- ✓ يمنع المستخدم من إزالة البرامج غير المرغوب فيها
- ✓ إقحام الإعلانات في أماكن لا توجد فيها عادة، مثل المواقع الحكومية
- ✓ عرض صفحات ويب لم تنوي زيارتها أو إرسال رسائل بريد إلكتروني لم تكتبها
- ✓ تظهر أشرطة أدوات أو أيقونات جديدة وغير متوقعة في المتصفح أو على سطح المكتب
- ✓ تحدث تغييرات غير متوقعة في المتصفح، مثل استخدام محرك بحث افتراضي جديد أو عرض علامات تبويب جديدة لم يفتحها المستخدم
- ✓ حدوث تغيير مفاجئ أو متكرر في الصفحة الرئيسية للإنترنت على جهاز الكمبيوتر

4-6-4 فهم كيفية الرد على سرقة الهوية والاحتيال والجرائم الإلكترونية

عند التعامل مع جرائم الإنترنت، يكون درهم وقاية خير من قنطار علاج، إذ تتسبب الجرائم الإلكترونية بأشكالها المختلفة، والتي تشمل سرقة الهوية عبر الإنترنت والاحتيال المالي والمطاردة والتنمر والقرصنة والخداع عبر رسائل البريد الإلكتروني والتزوير وجرائم الملكية الفكرية، في الإضرار بالضحايا وإزعاجهم وظهور العديد من المشاكل. ويمكن أن تؤدي جرائم الإنترنت في أسوأ الأحوال إلى خراب مالي وقد تهدد سمعة الضحية وأمنها الشخصي. لذا، يجب أن يتخذ المعلمون الإجراءات الملائمة لمنع الجرائم الإلكترونية والحفاظ على سلامة الطلاب وأمنهم باتباع إجراء "توقف"، "فكر" ثم "اتصل":



- ✓ اقفل تسجيل دخول الطلاب وقم بإنشاء حساب جديد من خلال اعتماد مصادقة قوية، مما يضيف طبقة أخرى من الحماية.
- ✓ قم بنسخ بيانات الطالب الشخصية وبيانات مكان العمل عن طريق عمل نسخ إلكترونية أو نسخ احتياطية من الملفات الأكثر أهمية.
- ✓ تعرف على الأجهزة المشتتة رقميًا، فأجهزة الكمبيوتر والهواتف المحمول هي ليست الأجهزة الوحيدة التي تحتجز وتخزن البيانات الشخصية الحساسة، فهناك أجهزة أخرى تحوي معلومات شخصية قيمة مثل الأقراص الصلبة وأجهزة USB وأجهزة الشرائط وذاكرة الفلاش المدمجة والأجهزة القابلة للارتداء ومعدات الشبكات وأدوات المكتب مثل آلات تصوير المستندات والطابعات وأجهزة الفاكس.
- ✓ قم بتفريغ سلة مهملات الطالب أو سلال المهملات على كل الأجهزة للتأكد من تدمير كل تلك الملفات، ومع ذلك لا يعد حذف وتفريغ سلة المهملات كافيًا لحذف الملفات كليًا، إذ يجب حذف الملفات بصفة دائمة، ومن ثم يتعين استخدام برنامج يقوم بحذف البيانات ومسحها من الجهاز ثم يستبدلها بوضع بيانات عشوائية بدلًا من معلوماتك - بحيث لا يمكن استرجاعها.
- ✓ يجب أن يتصل المعلمون بفريق الدعم الفني بالمدرسة ليتولى مسئولية الجهاز المصاب.

5-6-4 ما ينبغي على المعلمين معرفته حول تأمين حسابات الطلاب وأجهزتهم

1- ما هي بعض العلامات التي تشير إلى اختراق حسابات الطلاب على الإنترنت؟

- ✓ سيجد الطالب بعض المنشورات التي لم يقم بنشرها أبدًا على صفحة شبكة التواصل الاجتماعي الخاصة
  تكون منشورات تحث على النقر على أحد الروابط أو تحميل أحد التطبيقات.
- ✓ قد يخبرك أحد الأصدقاء أو أحد أفراد الأسرة بتلقي رسالة إلكترونية منك لم تقم بإرسالها أبدًا.
- ✓ وهذا يعني فقد معلوماتك بسبب انتهاك البيانات أو الإصابة ببرنامج خبيث أو فقد / سرقة الجهاز.

2- الخطوات التي ينبغي على المعلم القيام إذا اعتقد في اختراق أحد الحسابات

- ✓ أخبر كل جهات اتصالك أنهم قد يتلقون رسائل مزعجة يبدو أنها مرسلة من جانبك، وأخبرهم بألا يقوموا
  رسائل ولا ينقروا على أي روابط مرسلة من حسابك وحذرهم من احتمالية حدوث ضرر.
- ✓ وفي حالة اعتقادك بإصابة جهاز الكمبيوتر الخاص بك، تأكد من تحديث برنامج الأمان وقم بمسح النظام
  برامج خبيثة، وقم أيضًا باستخدام أدوات مسح وإزالة أخرى.
- ✓ قم بتغيير كلمات المرور لكل الحسابات التي تم اختراقها في أقرب وقت ممكن، ويجب ألا تقل كلمة المر
  12 حرف كي تكون قوية، وعليك باختيار جمل أو عبارات إيجابية يسهل تذكرها، على سبيل المثال
  موسيقى الريف". ويسمح في العديد من المواقع باستخدام المسافات.

قضايا وسائل التواصل الاجتماعي:

1- **تتوفر إعدادات الخصوصية والأمان لسبب ما:** تعرف على إعدادات الخصوصية والأمان بشبكات التواصل الا
وكيفية استخدمها، فتلك الإعدادات متوفرة للمساعدة في التحكم في مَن يرى المنشورات، كما تُدير استخدام
الإنترنت بطريقة إيجابية.

2- **النشر يعني النشر الدائم:** احمي سمعتك على شبكات التواصل الاجتماعي، فما يتم نشره من خلال شبكة الإنتر
دائمًا عليها، لذا فكر مليًا قبل نشر الصور التي لا تُود أن يراها والديك أو أصدقاؤك في المستقبل.

3- **قد تتمتع بسمعة طيبة على الإنترنت:** أكدت البحوث التي أُجريت مؤخرًا أن شركات التوظيف تستجيب لأي
تجارية شخصية قوية وإيجابية عبر الإنترنت، حيث إنها تُظهر مدى ذكائك وطريقة مراعاتك لمشاعر الغير
حرصك على البيئة.

4- **الاحتفاظ بالبيانات الشخصية:** توخى الحذر بشأن مقدار المعلومات الشخصية التي تعرضها على مواقع شبكات التواصل الاجتماعي، فكلما زاد مقدار البيانات المنشورة أصبح من السهل على أي مخترق أو أي شخص آخر استخدام هذه المعلومات لسرقة هويتك أو الوصول إلى بياناتك أو ارتكاب جرائم أخرى كالتلصص.

5- **معرفة أصدقائك وإدارتهم:** تُستخدم شبكات التواصل الاجتماعي لأهداف متعددة، فتكوين مجموعة كبيرة من الأصدقاء أمر مستحسن في العديد من جوانب الحياة، وهذا لا يعني بالضرورة أن يكونوا متساويين، لذا استخدم أدوات إدارة المعلومات التي أطلعت أصدقاءك عليها في مجموعات مختلفة أو حتى على صفحاتك المتعددة عبر الإنترنت، وعند محاولة خلق شخصية عامة كمدون أو خبير قم بإنشاء ملف تعريف عام أو صفحة "معجبين" تشجع على المشاركة الواسعة، وتحد من مقدار المعلومات الشخصية المنشورة، واستخدم ملفك التعريفي الشخصي لإبقاء أصدقائك الحقيقيين (الذين تعرفهم وتثق بهم) على اطلاع بكل جديد في حياتك اليومية.

6- **كن صادقًا عند شعورك بالانزعاج:** إذا قام أحد الأصدقاء بنشر شيء عنك جعلك تشعر بالانزعاج أو يبدو أنه غير لائق، بأبلغه بذلك، وبالمثل كن منفتحًا إذا أخبرك أحد الأصدقاء بأن ما نشرته عنه جعله يشعر بالانزعاج، وتتفاوت درجة التسامح لدي بعض الأفراد فيما يتعلق بما يعرفه الغير عنهم؛ لذا يجب عليك احترام تلك الاختلافات.

7- **تعرف على ما يتعين اتخاذه من إجراءات:** إذا قام شخص ما بمضايقتك أو تهديدك فاحذفه من قائمة الأصدقاء وأحظره وإبلاغ مسؤول الموقع عنه.

احم نفسك من باتباع إجراء: توقف وفكر واتصل:

- ✓ **تملك تواجدك على شبكة الإنترنت:** اضبط إعدادات الخصوصية والأمان على مواقع الويب وفقًا لما تراه مناسبًا لك لمشاركة المعلومات عند الاقتضاء، ثم حدِّد كيف ومع مَن تفضل مشاركة المعلومات.
- ✓ **اجعل عبارة المرور جملة:** تتكون عبارة المرور القوية من جملة من 12 حرفًا على الأقل، وننصح بالتركيز على الجمل أو العبارات الإيجابية التي تحب التفكير فيها ويسهل تذكرها (على سبيل المثال "أنا أحب موسيقى الريف")، ويمكن حتى استخدام المسافات في العديد من المواقع!
- ✓ **حساب فريد وعبارة مرور فريدة:** يساعد اختلاف عبارات المرور بين الحسابات على إحباط محاولات مجرمي الإنترنت على اختراق الحساب، وعلى أدنى تقدير استخدم عبارة مرور مختلفة لكل من حسابات العمل والحسابات الشخصية، وتأكد من تعيين عبارة مرور قوية للحسابات الهامة.
- ✓ **عندما ترتاب في منشور احذفه فورا:** يحاول مجرمو الإنترنت سرقة المعلومات الشخصية من خلال روابط البريد الإلكتروني والتغريدات والمنشورات والإعلانات، فإذا كان هنالك منشور يثير الريبة -حتى عندما يكون المصدر معروفًا- فاحذفه على الفور.

- ✓ **فقط انشر عن الغير ما تفضل أن ينشره عنك**

تأمين أجهزة المحمول:

- ✓ يحتوي الهاتف الذكي أو الجهاز اللوحي أو الكمبيوتر المحمول على معلومات هامة عنك وعن أصدقائك وعائلتك بما في ذلك أرقام الاتصال والصور والمواقع.
- ✓ ويتعين عليك حماية جهازك المحمول، وعليه يجب تطبيق احتياطات الأمان التالية كي تستخدم الوسائل التقنية دون أن يساورك أي قلق.

تثبيت برنامج أمان:

- ✓ **حدث برنامج الأمان دائمًا على جميع الأجهزة المتصلة بالإنترنت:** يُعد الحصول علي أحدث إصدارات برامج تأمين الأجهزة المحمولة ومتصفحات الويب وأنظمة التشغيل والتطبيقات بمثابة أفضل وسائل دفاع ضد الفيروسات والبرامج الضارة والتهديدات الأخرى عبر الإنترنت.
- ✓ **حذف عند الانتهاء:** يُحمل الكثير التطبيقات لهدف محدد كالتخطيط لقضاء أجازات، ويحبذ حذف هذه التطبيقات عند عدم الحاجة إليها.
- ✓ **حماية المعلومات الشخصية:** المعلومات الشخصية قيِّمة للغاية، لذا احمها! فالمعلومات الشخصية كالألعاب التي تفضلها وما تبحث عنه عبر الإنترنت وأماكن التسوق والإقامة ذات قيمة لا تقل عن قيمة المال، وعليه فكر مليًّا في من يمكنهم الحصول على هذه المعلومات، وكيف تُجمع من خلال التطبيقات والمواقع الإلكترونية، وحاول ألا تنشر الكثير من المعلومات الشخصية عبر الإنترنت، **فقد تقع المعلومات في أيدي غير أمينة إذا لم تُدار بعناية.**
- ✓ **تأمين الأجهزة:** استخدم عبارات أو رموز مرور قوية، أو خاصية أخرى كالمعرّف اللمسي لقفل أجهزتك، ويساعد تأمين جهازك على حماية ما عليه من معلومات حال فقدانه أو سرقته، وذلك أيضًا يجعلها في منأى عن أعين المتطفلين.
- ✓ **إدارة مشاركتك على شبكة الإنترنت:** استخدم إعدادات الأمان والخصوصية على مواقع الويب والتطبيقات لإدارة ما تشاركه ومن يمكنه رؤية ما تشارك.
- ✓ **تواصل بحذر:** عندما ينتابك شك في أمر فلا تستجيب له، حيث تتزايد الرسائل النصية والمكالمات والبريد الصوتي الاحتيالية، وكالبريد الإلكتروني تصل إليك طلبات عبر الهاتف المحمول للحصول على بيانات شخصية أو القيام بإجراء فوري ما، وهي من أساليب الاحتيال.

7-4 الاستجابة لمخاطر البث المباشر

1-7-4 البث المباشر؟

البث المباشر هو بث فيديو مباشر في الوقت الحقيقي للجمهور من خلال شبكة الإنترنت، فكل ما تحتاجه لبث فيديو مباشر هو جهاز يدعم الإنترنت -كهاتف ذكي أو جهاز لوحي- ومنصة للبث، ويمكن تشبيه ذلك بمذيع أو مراسل صحفي يبث الخبر "من قلب الحدث"، حيث أصبحت عبارة "أنت على الهواء مباشر من فضلك لا تسب!" شائعة، ويمثل البث المباشر أمرًا جذابًا جدًا للشباب، حيث يتم مُشاهدتهم من قِبل جمهور كبير محتمل، مما يتيح لهم الفرصة لأن يكونوا ومنتجين ومقدمين، ويمكن بث أي أمر تقوم به في جميع أنحاء العالم دون تأخير أو تعديل، ونظرًا لشعبية وشهرة منصات البث المباشر مثل Snapshots وYouNow وLive.ly أطلقت منصات وسائل التواصل الاجتماعي التقليدية خاصية البث المباشر، فعلى سبيل المثال لا الحصر طرح فيسبوك خاصية البث المباشر على فيسبوك، بينما أطلق تويتر برنامج بيريسكوب، ويمثل الحفاظ على الذات أمرًا هامًا حقًا للطلاب، حيث تعزز مشاركتهم لحدث ما وجذب اهتمام الناس أثناء البث المباشر الشعور بالثقة المطلقة والغرور.

2-7-4 ما فرص ومخاطر البث المباشر؟

يساعد التفكير في الدافع وراء عمليات البث المباشر في مراعاة مراحل تطور الطالب، وتمثل المحافظة على الذات أمرًا هامًا حقًا للطلاب، حيث تعزز مشاركتهم لحدث ما وجذب اهتمام الناس أثناء البث المباشر الشعور بالثقة المطلقة والغرور، 4ذ0فالتفاعل الإيجابي الفوري من خلال بداء "الإعجابات" والتعليقات الإيجابية يحفز الشعور بالسعادة في أدمغة المراهقين، وتتيح عمليات البث المباشر لطفلك مشاهدة البث "المباشر" وكذلك بث فيديو مباشر لنفسه، ولكن هناك مخاطر يجب أن تكون على دراية بها في كلا النشاطين، فقد يكون الفيديو المباشر مزيفًا؛ لذا شجع طفلك على التفكير مليًا في معرفة السبب وراء رغبة شخص مجهول في الدردشة معه، وإذا كان الموقع يحتوي على إعدادات للخصوصية فتأكد دائمًا من أن أطفالك يستخدمونها للتحكم في مَن يمكنه التواصل معهم.



يجب أن يكون المعلمون على دراية بالحقائق التالية حول البث المباشر:

1- يجب أن لا يقل عمر المستخدم عن 13 عامًا حتى يتثنى له استخدام التطبيق، كما يُنصح الطلاب بالحصول على إذن من والديهم قبل تنزيل التطبيق.

2- تتوفر التطبيقات حاليًا على الهواتف الذكية فقط.

3- تسمح التطبيقات للأشخاص بالبث المباشر وبث ما يقومون به في أي وقت، ونظرًا لأن المحتوى يُبث مباشرة فإنه ليس خاضعًا للإشراف حتى يتمكن البالغين من التحدث مباشرة مع الطلاب الشباب.

4- يقوم الطالب بإرسال رسائل بريد إلكتروني وتقديم لقطات شاشة للإساءة كدليل عند رغبته في الإبلاغ عن إساءة أو تلقيه رسائل غير مناسبة.

5- تُشارك مقاطع الفيديو موقع الطالب، كما تتيح للمستخدمين البحث عن جهات بث أخرى في نفس المنطقة.

إرشادات المعلمين لحماية الطلاب من مخاطر البث المباشر:

1- تحدث دائمًا مع الطلاب

2- انصحهم بحماية معلوماتهم الشخصية قبل البث.

3- توصل لاتفاق معهم بشأن استخدام الجهاز

4- علم الطلاب متى يقولون "لا"

5- شجع الطلاب على الإبلاغ عن أي محتوى سيء، واشرح لهم كيف يمكنهم الإبلاغ عن مواد مسيئة على المنصة المستخدمة للبث المباشر

القسم 5: يحتاج المعلمون إلى معرفة المشكلات الأولية لإدارة أمان الطلاب عبر الإنترنت

5-1 الإنصات الإيجابي

5-1-1 الإنصات الإيجابي: الأساسيات

قد يكون الإنصات الإيجابي أداة قوية لتحسين التواصل وبناء علاقة إيجابية مع الطلاب، كما أنه أكثر من مجرد الاستماع لهم، فهو بمثابة مهارة.

يمكن تطبيق الإنصات الإيجابي من خلال:

- ✓ الاقتراب من الطالب عندما يتحدث.
- ✓ إيلاء الطالب الاهتمام الكامل.
- ✓ السماح للطالب بالتحدث دون مقاطعة.
- ✓ تجنب طرح الأسئلة التي تقطع تسلسل الأفكار.
- ✓ التركيز على ما يقوله الطالب بدلاً من التفكير فيما ستقوله بعد ذلك.
- ✓ النظر إلى الطالب حتى يعلم أنه يتم سماعه وفهمه.
- ✓ إظهار الاهتمام بحديث الطالب من خلال الإيماءة برأسك وإبداء التعليقات مثل "أتفهم ذلك"، هذا يبدو قاسيًا / رائعًا / صعبًا...".

5-1-2 فوائد الإنصات الإيجابي

يمكن للمعلم تعزيز التواصل مع الطلاب وتحسين علاقته معهم من خلال الإنصات الإيجابي، وذلك لأن الإنصات الايجابي يُظهر للطالب أن المُعلم مهتم بما يقوله، وكذلك يساعد المُعلم على معرفة المزيد عن ما يحدث في حياة الطالب وفهمه، وكون المُعلم مُنصتًا لن يكون هنالك داعي للحديث بكثرة، كما يقلل أيضًا من الضغوط التي تقع على عاتق المُعلم للتوصل إلى إجابات للمشكلات وحلها، كما أنه يجعل من المرجح أن يسأل الطالب المُعلم عن رأيه.

5-1-3 تحسين مهارات الإنصات الايجابي

1- **الإصغاء الجيد:** يجب على المعلم أن يُصغي جيدًا لما يقوله الطالب وأن يعيره كامل اهتمامه، فذلك يبعث برسالة إلى الطالب مفادها أنه أهم شخص، وأن المُعلم مهتم بحديثه وبما يشعر به وبما يفكر فيه وبما يفعله.

2- **محاولة الفهم:** ركز على ما يقوله الطالب بدلاً من التفكير فيما ستقوله بعد ذلك، فهل فاتتك وجهة نظره بتفكيرك في وجهة نظرك أنت؟ وما الذي يحاول أن يخبرك ولماذا؟

3- **إظهار أنك تحاول فهمه:** لخص النقاط الرئيسية للطالب وما تعتقد أنه يشعر به، وحاول تكرار ما قاله الطالب بطريقتك، على سبيل المثال "دعني أوضح ما إذا كنت قد فهمت حديثك بشكل صحيح أم لا، فأنا ألاحظ أنك تشعر بالغضب لأنني لم أتحدث إليك قبل وضع خطط لعطلة نهاية هذا الأسبوع. أستطيع تفهم ذلك." فعندما يكون الشخص منصتًا إيجابيًّا، ويكرر ما قاله الطالب فإن ذلك يحث الطالب على قول المزيد لأنه يشعر بأنه كل ما قاله تم الإصغاء له بعناية، كما يمكن أن يشجعه على شرح أو الإدلاء بالمزيد حول ما يفكر فيه الطالب.

5-1-4 استراتيجيات حل المشكلات مع الطلاب

العمل مع الطلاب على إيجاد حلول للمشاكل يمكن أن يعزز المرونة في التعامل معها أيضًا، وقد يساعد وجود استراتيجيات لحل مشكلات الطلاب على الشعور بأن لديهم القدرة على التعامل مع المواقف والأوقات الصعبة وتجاوزها، ويُعد حل المشكلات مهارة حياتية هامة يجب على الطلاب اكتسابها، ويساعد كل من التواصل الهادئ والإنصات الايجابي والحل الوسطي المعلمين في إيجاد حل للمشكلات مع طلابهم، وعند حل المشكلات من الجيد أن تكون قادرًا على:

- ✓ الإنصات والاستماع بهدوء.
- ✓ مراعاة الخيارات المتاحة واحترام أراء الآخرين ومتطلباتهم.
- ✓ البحث عن حلول بناءة وإيجاد حلول وسطية أحيانًا.

من الهام أيضًا أن يتحدث الطالب عن ما يشعر به من الخوف أو القلق أو الغضب، كما يجب أن يكون لديه إستراتيجيات بسيطة لتحويل الحالات المزاجية السيئة إلى جيدة، وفيما يلي بعض الأفكار:

- ✓ قم بالأمور التي تستمتع بها أو التي تساعدك على الاسترخاء، مثل مشاهدة برنامج تلفزيوني مضحك أو فيلم على قرص دي في دي أو قراءة كتاب جيد.
- ✓ قضاء بعض الوقت مع الأصدقاء أو في مساعدة الأفراد.
- ✓ اصنع شيئًا لطيفًا لشخص أخر.
- ✓ ابحث عن الجوانب الإيجابية أو الممتعة في المواقف الصعبة، على سبيل المثال يؤدي التواء الكاحل إلى عدم ممارسة الرياضة في عطلة نهاية الأسبوع، ولكنه يمنحك فرصة لمشاهدة مسلسلات التلفاز المفضلة لديك.
- ✓ مارس بعض الأنشطة البدنية مثل الألعاب الرياضية أو المشي بخطوة سريعة.
- ✓ استرجع بعض الذكريات الجيدة من خلال رؤية الصور.

2-5 الثقة في الطلاب

1-2-5 أسباب أهمية بناء الثقة لدى الطلاب

تساعد الثقة الطلاب على تصفح الإنترنت بصورة آمنة واتخاذ قرارات مستنيرة وتجنب الأشخاص والمواقف التي لا تناسبهم، فلكي يشعر الطلاب بالثقة يجب أن تكون علاقتهم قوية بالمعلمين، كما أن الثقة هي الاعتقاد بأن الطالب سوف يكون ناجحًا أو يقوم بالاختيار الصحيح في موقف معين، فهي تتعلق بتقدير بالذات؛ وهو بمثابة الشعور بالرضا عن النفس والشعور بأنه شخص جدير بالاهتمام، ولكن شدة تقدير الذات لا تعكس أن الطالب سيشعر دائمًا بالثقة، كما تتعلق الثقة بالمرونة أيضًا، فالمرونة هي القدرة على تجاوز التجارب الصعبة والتصدي للمواقف العصيبة، وسيشعر الطالب بمزيد من الثقة في التعامل مع المواقف الصعبة إذا كان يتمتع بالمرونة وكان قادرًا على التغلب على الصعوبات عندما تصبح الحياة عصيبة، فتلك دورة إيجابية، كما أن الثقة تساعد الطلاب على اتخاذ قرارات آمنة ومستنيرة، فيمكن للطلاب الواثقين من أنفسهم تجنب الأشخاص والمواقف التي لا تناسبهم والاضطلاع بالأنشطة التي تناسبهم، إذا كان الطالب واثقًا من نفس، فمن الأرجح أن يكون حازمًا وإيجابيًا ومثابرًا ومتحمسًا وطموحًا.

5-2-2 كيفية بناء الثقة والمرونة لدى الطلاب

فيما يلي بعض النصائح لبناء الثقة والمرونة لدى الطلاب:

1- **العملية:** ابحث عن الأمور العملية والإيجابية التي يمكن للطالب القيام بها لبناء مهاراته وزيادة فرص نجاحه، ويمثل إعطاء الطالب إستراتيجية واضحة لتحسين احتمالية نجاحه طريقة رائعة لمساعدته على فهم ما يمكنه القيام به لتحقيق أهدافه.

2- **منح الطلاب فرص لتجربة أمور جديدة:** عندما يجرب الطلاب أمور مختلفة سيتعرفون على ما يجيدونه وما هو ممتع، فمعظمهم يجيدون القيام ببعض الأمور ولا يجيدون القيام بالبعض الأخر - وهذا أمر جيد، فلا يمكننا أن نكون جميعًا رياضيين أولمبيين أو أبطال ألعاب أو عباقرة موسيقية.

3- **تشجيع الطلاب على الاستمرار في المحاولة:** إذا فشل الطالب في القيام بأمر ما ساعده في فهم أن الجميع يرتكبون أخطاء، وأخبره أن يستمر في المحاولة فلا بأس من عدم تحقيق الأمر من المرة الأولى، كما يمكن للمعلمين مشاركة الطلاب لبعض الأمثلة عن الأوقات التي فشلوا فيها أو حين كانوا بحاجة إلى من يقدم لهم المساعدة أو حين كانوا يتعين عليهم المحاولة مرة أخرى.

4- **القدوة:** يمكن للمعلمين أن يكونوا قدوة عندما يتعلق الأمر بالثقة، حيث يمكنهم إعداد متحدثين جيدين، كما يفضلون مشاركة معلوماتهم الوفيرة مع الطلاب.

5- **تشجيع الطلاب على التصرف بثقة**: اطلب من الطلاب القيام بمشاريع تتطلب منهم تقديم موضوعات مختلفة وإنشاء نماذج يحتذون بها أو تصميمها.

6- **ممارسة المهارات الاجتماعية:** يحتاج الطالب إلى بعض الإرشادات من المعلم في حالة شعوره بالقلق في المواقف الاجتماعية.

7- **الثناء على مجهود الطلاب:** حاول أن تثني على الجهود المبذولة من الطالب في النشاط في حالة إخفاقه في امتحان أو مقابلة أو لعبة بدلاً من التركيز على النتيجة، اقترح عليه بعض الأفكار حول ما يمكنه القيام به بطريقة مختلفة في المرة القادمة.

5-2-3 تقديم المساعدة من أجل زيادة الثقة لدى الطالب

تحدث مع الطالب كخطوة أولى إذا تغيرت ثقته في نفسه فجأة أو إذا منعته ثقته الضعيفة في نفسه من تجربة أمور جديدة، وذلك سيساعد على معرفة ما يحدث، واطلب من الوالدين تقديم المساعدة في حالة عدم قدرتك على تقديمها.

فيما يلي مقترحات لتعزيز ثقة الطالب:

1- اطرح مواضيع للمناقشة.

2- كن إيجابيًّا.

3- شجع على تقييم الذات والأقران.

4- قدم ملاحظات مفيدة.

5- حثهم على التخلص من الأفكار السلبية.

6- اشرح لهم أن بذل الجهود أمر طبيعي.

3-5 حالة الطالب المزاجية: التغيرات المزاجية أثناء سن البلوغ

1-3-5 ما الذي يحتاج المعلمون إلى معرفته عن الحالة المزاجية؟

يستطيع المعلمون مساعدة الطلاب على إدارة التقلبات العاطفية والتغيرات المزاجية بطرق عديدة منها التواصل مع طلابهم، وقد يلاحظ المُعلم أن الطالب أكثر سعادة أو حزنًا من المعتاد بل وأكثر من ذلك بكثير، وقد يرجع ذلك لأسباب عديدة -جسدية وعاطفية واجتماعية ونفسية- ولا يوجد سبب بعينه على وجه الخصوص، كما لا يمكنك تحديد سبب واحد لتقلبات الحالة المزاجية للمراهقين غالبًا، وقد يلاحظ المعلم أيضًا تغير العلاقة بينه وبين الطالب، وأنه أصبح أكثر عاطفية من ذي قبل.

2-3-5 يجب على المعلمين محاولة فهم الحالة المزاجية للطالب.

1- **العوامل الجسدية: قد يكون الطالب بحاجة إلى النوم أو الطعام، وقد يكون هنالك مشاكل تتعلق بسلامة البيئة المنزلية للطالب وأمنها.**

2- **عوامل ذهنية:** يرتبط قسم الدماغ الذي ينمو أخيرًا -المعروف بالقشرة الأمامية الجبهية- ارتباطًا وثيقًا بالمناطق المسؤولة عن تنظيم العواطف والسيطرة عليها، وهذا يدل على أن الطلاب قد يجدون صعوبة في التحكم في بعض عواطفهم الجياشة، وقد يبدو أنهم يتفاعلون بحماس أكبر مع المواقف أكثر من المعتاد، كما أنهم لا زالوا يتعلمون معالجة هذه المشاعر والتعبير عنها بطريقة ناضجة.

3- **العوامل العاطفية والاجتماعية:** يمكن أن تكون الأفكار الجديدة والعواطف والأصدقاء والمسؤوليات كلها عوامل، كما أن الطلاب لا يزالون يتعلمون كيفية إيجاد حلول للمشكلات من تلقاء أنفسهم ودون مساعدة، ويسعون نحو الاستقلال، وقد يكون الطالب أيضًا منشغلًا كثيرًا بالتفكير في التحديات التي يوجهها مثل إنشاء الصداقات والعلاقات المدرسية والعائلية في ظل تغير الهرمونات الجسدية، ولكن فقط حاول أن تتأكد من أن الحالة المزاجية ليست مرتبطة بمضايقات أو تنمر إلكتروني.

5-3-3 دور المعلمين عند التعامل مع عواطف الطلاب

1- **مساعدة الطلاب على فهم الحالة المزاجية:** اشرح للطالب أنه من الطبيعي أن يكون هناك تقلبات مزاجية عاطفية.

2- **البقاء على تواصل مع الطلاب:** ابق على تواصل مع الطلاب وأنصت إليهم لمعرفة إلى ما يحدث معهم، فقد يساعد ذلك المعلم على فهم الحالة المزاجية للطالب، وإذا ظلت هذه المشاعر قائمة لفترة فمن الأفضل التحدث مع أولياء الأمور لمعرفة السبب.

3- **منح الطلاب مساحة شخصية:** يحاول الطلاب الاستقلال من خلال القيام بأمور جديدة، لذا حاول منحهم مساحة شخصية أو بعض الوقت بمفردهم للتفكير في المشاعر والخبرات الجديدة.

4- **تأجيل الحلول:** ناقش حلول للمشكلات مع الطالب لكن دعه يساهم في تلك الحلول كي يتمكن من حل المشكلة، فعادة ما يفضل الطالب أن يشارك في حل مشاكله الخاصة، ويمثل حل المشكلات أيضًا مهارة حياتية قيمة يصقلها الطالب من خلال محاولة حل مشاكله، لذا ساعده وحثه على تطوير مهارة حل المشكلات، وبهذه الطريقة ترسل رسالة مفادها أن مساهمة الطالب في حل المشكلات أمر ضروري.

5- **العمل معًا على إستراتيجيات المواجهة:** يمثل تعلم كيفية التعامل مع تقلبات الحالة المزاجية العاطفية وإدارتها بصورة مستقلة واحدة من المهام الكبرى في مرحلة المراهقة، ويستطيع المعلم مساعدة الطلاب على تطوير هذه المهارة الحياتية المهمة.

5-4 المواطنة الرقمية: كيف يكون المراهقون مسؤولين علي الإنترنت

5-4-1 فهم المواطنة الرقمية المسؤولة

المواطنة الرقمية:

- ✓ يكون الطالب مواطنًا رقميًا إذا كان لديه هاتف ذكي أو حساب على وسائل التواصل الاجتماعية أو يستخدم منصة تعليمية عبر الإنترنت أو ينشئ محتوى رقمي.
- ✓ تعني المواطنة الرقمية المسؤولة المشاركة في حياة المجتمع الإلكتروني بطريقة آمنة وأخلاقية ومحترمة.
- ✓ يتصرف المواطنون الرقميون باحترام، ويحمون سمعتهم وخصوصيتهم، وينتبهون لأسلوبهم ولهجتهم، كما تساورهم الشكوك دائمًا.

أن تكون مواطنًا رقميًا مسؤولًا يعني أن لديك مهارات اجتماعية على الإنترنت للمشاركة في الحياة المجتمعية الإلكترونية بطريقة أخلاقية ومحترمة، ويُقصد بالمواطنة الرقمية المسؤولة:

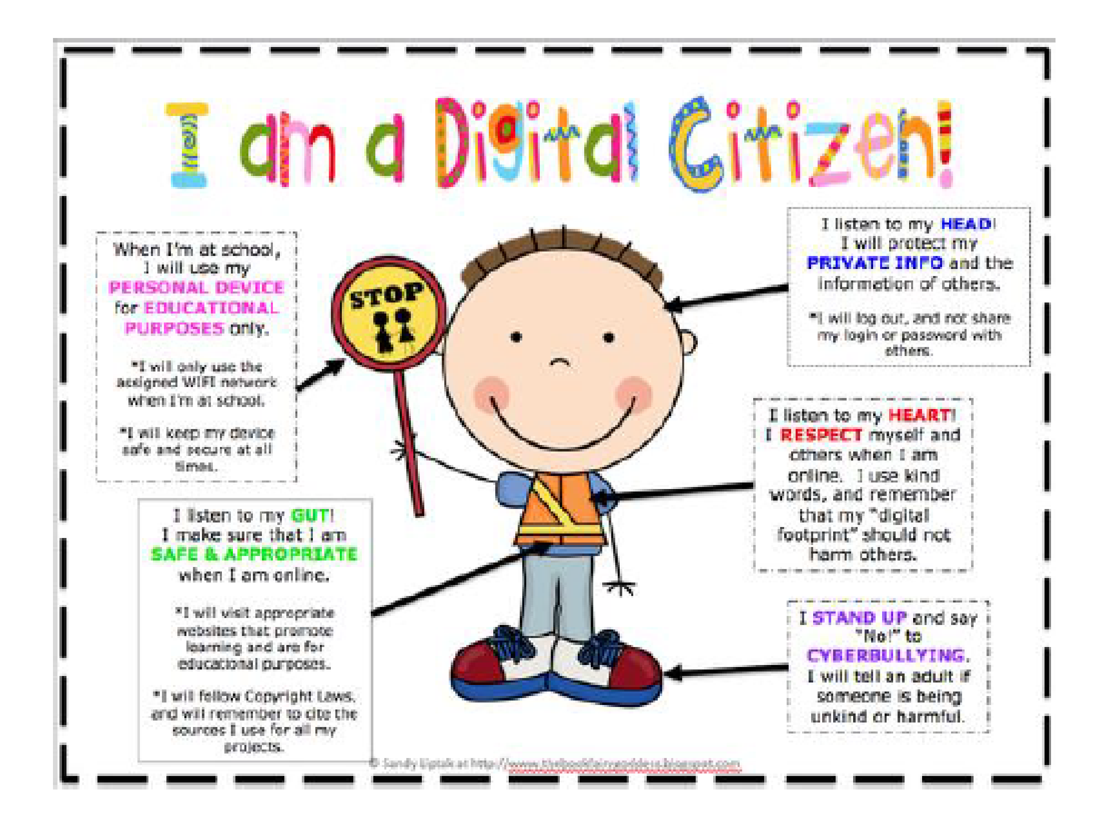
- ✓ التصرف بطريقة قانونية، حيث يُعد الاختراق أو السرقة أو التنزيل غير القانوني أو إتلاف عمل أشخاص آخرين أو هويتهم أو ممتلكاتهم عبر الإنترنت جريمة يحاسب عليها القانون.
- ✓ حماية خصوصيتك وخصوصيات الآخرين.
- ✓ معرفة حقوقك وواجباتك عند استخدام الوسائط الرقمية.
- ✓ التفكير في كيف تؤثر الأنشطة الإلكترونية عليك وعلى والأصدقاء والأقارب ومجتمع الإنترنت على نطاق واسع.

2-4-5 كيف تكون مواطنًا رقميًا مسؤولاً وآمنًا

فيما يلي بعض الطرق لتشجيع الطلاب على أن يكونوا آمنين ومسؤولين على الإنترنت:

1- **بادر بالاحترام وتوقع معاملة بالمثل:** علم الطلاب احترام أنفسهم والآخرين، حيث يمثل ذلك أمرًا هامًا في جميع العلاقات، ولا يختلف عندما يكون الطلاب متصلين بالإنترنت، وعليه يجب على المعلمين تشجيع طلابهم على التعامل مع الأصدقاء عبر الإنترنت بنفس القدر من الاحترام الذي يتلقونه وجهًا لوجه، ولا يُسمح لك -كونك مواطنًا رقميًا مسؤولاً- بإنشاء أو إعادة توجيه رسائل البريد الإلكتروني أو الصور أو الرسائل النصية السيئة أو المهينة عن الآخرين.

2- **حماية سمعة الطالب:** تأكد من أن الطلاب على دراية بالعواقب التي تنتج جراء نشر صور ومقاطع الفيديو وتحميل محتوى شخصي آخر، فبمجرد نشر هذا المحتوى على الإنترنت يكون من الصعب للغاية حذفه، وقد يصبح جزءًا من سمعة الطالب الدائمة عبر الإنترنت، فعلى سبيل المثال قد تقول: "قد تبدو بعض الصور ومقاطع الفيديو جيدة بالنسبة لك الآن، ولكن قد تشعر بشعور مختلف حيالها مستقبلاً، ولا ترغب في رؤية الأشخاص لها"، وقد يوافق المعلم على أن يعرض الطلاب منشوراتهم وصورهم ومحتوياتهم الأخرى قبل تحميلها وذلك بناء على أعمارهم.



3- **حماية الخصوصية:** هناك عدة طرق يمكن للطلاب من خلالها حماية خصوصيتهم:

- ✓ مشاركة جزء من المعلومات الشخصية حسب الضرورة - على سبيل المثال ليس من الضروري إدخال تاريخ الميلاد أو أرقام الهواتف المحمولة أو عناوين البريد الإلكتروني أو المدن على كافة مواقع الإنترنت.
- ✓ تحديث إعدادات الخصوصية على مواقع التواصل الاجتماعي باستمرار، بحيث لا تكون ملفات تعريف الطلاب متاحة للعامة.
- ✓ عدم اطلاع أي شخص على كلمات المرور.
- ✓ التحقق من إعدادات الموقع والخدمات على الهواتف الذكية والأجهزة اللوحية والتطبيقات، ويمكن القيام بذلك عادةً عن طريق الانتقال إلى "الإعدادات" أو التحقق من إرشادات تشغيل الجهاز أو التطبيق، قم بإيقاف تشغيل خدمات تحديد الموقع التي لا يحتاجها الطالب.

4- **الحرص:** من المهم أن يكون الطلاب حذرين بشأن ما يشاركونه مع أشخاص لا يعرفونهم، كما يجب أن يكون المعلمون على دراية بالمواقع التي تساعد على تجنب عمليات الاحتيال مثل (https://www.hoax-slayer.net/)، ويجب على الطلاب أيضًا توخي الحذر عند النقر فوق النوافذ المنبثقة على مواقع الويب، حيث قد تنقلك بعض النوافذ المنبثقة التي تبدو آمنة إلى مواقع إباحية أو تطلب منك معلومات شخصية.

5-5 المرونة الرقمية لدى الطلاب:

1-5-5 ما يجب على المعلمين معرفته

يتعامل الطلاب بصورة أفضل في المواقف العصيبة أو بعدها عندما يكونوا مرنين، وذلك نظرًا لأن لديهم القدرة على "التعافي" عندما تسوء الأمور، ويحتاج الطلاب إلى أن يكونوا مرنين لمواكبة الظروف الحياتية المتغيرة، وبالتالي فإن بناء تلك القدرة أمر هام للتطور، فالمرونة تُعرف بـ "التعافي" خلال الأوقات الصعبة أو بعدها، والعودة إلى سابق العهد، وتعرف أيضًا بالقدرة على التكيف مع الظروف الصعبة التي لا يمكن للفرد تغييرها وتظل تتفاقم، وفي الواقع عندما يكون الشخص مرنًا يمكنه في كثير من الأحيان التعلم من المواقف الصعبة التي يمر بها، ويستطيع جميع الطلاب أن يكونوا مرنين من خلال تطوير المواقف السلوكية مثل احترام الذات والمهارات الاجتماعية والتنظيمية وعادات التفكير الإيجابي، كما أنها تُعرَّف أيضًا بقدرة الفرد على التكيف بصورة دقيقة مع المتغيرات وأحيانًا البيئات المسببة للإجهاد والشعور بالقدرة على التصرف واتخاذ قرارات مستنيرة عوضًا عن الاستسلام في مواجهة التحديات الجديدة والتهديدات، وبالتالي من أجل تطوير هذه القدرة لدى الطلاب ليس من الجيد أن يكون لديك استراتيجيات مقيدة لحل المشكلات التي يواجهوها في حياتهم بصورة صريحة، وبدلاً من ذلك قم بإنشاء نظام يعمل على تطوير قدرة الطالب على إيجاد حلول للمشكلات والتصرف في المواقف الحرجة وعند موجة المخاطر وتوجيه الذات وتنمية المهارات اللازمة لتخفيف المخاطر التي يواجهها عبر الإنترنت، ويتعلم الطلاب بشكل أفضل طرق مواجهة المخاطر والتعامل معها في سياق داعم لهم ومتعاطف معهم، مما يترتب عليه شعورهم بالأمان، كما يجب عدم الحكم عليهم بقسوة عندما يرتكبون أخطاء، ويجب توفير مثل تلك السياقات في المنزل والمدرسة وكذلك في البيئة الرقمية نفسها.

- ✓ يجب تطوير المرونة الرقمية؛ وذلك نظرًا لأن الطلاب يمكنهم بالتالي أن يعيشوا كوكلاء نشطين، كما يجب أن يكونوا قادرين على ممارسة ضبط النفس والحكم المستقل بأمان ومسؤولية.
- ✓ وتختلف وجهة نظر الطالب وإدارته للمخاطر بشكل كبير عن وجهة نظر البالغين.
- ✓ يعتمد تصور الطالب للمخاطر على تقييمهم للبيئة الإلكترونية وعواقبها المحتملة، بما في ذلك معرفة فرص تقديم الدعم والتعويض.
- ✓ تميل إستراتيجيات المعلمين وأدوات التقنية المتاحة بشكل كبير إلى معالجة المخاطر المتعلقة بالمحتوى، مع التركيز بدرجة أقل على القضايا مثل التنمر على الإنترنت والاستدراج وإرسال الصور ومقاطع الفيديو غير المناسبة والمضايقات الإلكترونية.

5-5-2 أسباب حاجة الطلاب للمرونة

يحتاج الطلاب إلى المرونة للتغلب على **التحديات اليومية** مثل كالخلافات والمجادلات مع الأصدقاء أو نتائج الاختبارات المحبطة أو الخسائر الرياضية، كما يواجه بعضهم تحديات أكثر خطورة مثل التنمر، ويواجه البعض الآخر تحديات أكثر من غيرها بسبب صعوبات التعلم أو الإعاقات، أو لأن لديهم شخصيات منزعجة وقلقة، وعليه فإن المرونة تساعدهم على مواجهة هذه التحديات، ومن الواضح أن أقلية من الطلاب أكثر تعرضًا للإساءة عبر الانترنت من غيرهم، ويمكن للمعلم مساعدة الطلاب على تعلم كيفية استخدام الإنترنت بأمان ومسؤولية، وإذا تم تعليم الطلاب كيفية إدارة مخاطر السلامة على شبكة الإنترنت والظروف المثيرة للقلق سوف يتمكنون من بناء ما يسمى بالمرونة الرقمية، حيث سيكون بمقدورهم التعامل مع أي مخاطر يواجهونها عبر الإنترنت ومواجهتها بصورة إيجابي.

يمكنك القيام بذلك عن طريق:

- ✓ التواصل مع الطلاب عبر الإنترنت.
- ✓ التحدث مع الطالب حول المحتوى المتاح على شبكة الانترنت.
- ✓ أن تكون قدوة جيدة.
- ✓ تعليم الطالب أن يكون حذرًا عند الكشف عن معلوماته الشخصية.
- ✓ حث الطالب على تجنُّب الشراء عبر الإنترنت.
- ✓ التحدث مع الطالب عن السلوك المناسب الذي يجب اتباعه عند استخدام الإنترنت.

5-5-3 القيم والمواقف الشخصية لبناء المرونة

1- **احترام الذات:** يمثل ذلك حجر الزاوية في عملية بناء المرونة، ويمكن تنمية احترام الذات عن طريق وضع معايير للسلوك، فإذا كان الطالب يحترم ذاته سيؤمن أنه ذو شأن، ويجب معاملته باحترام من قِبل الآخرين، وكذلك يكون الطالب أكثر قدرة على حماية نفسه من خلال تجنب السلوكيات والمواقف الخطرة، كما أن الشعور القوي باحترام الذات يساعد الطالب على أن يكون أقل عرضة للتنمر والمضايقات.

2- **التعاطف واحترام الغير والرأفة والإنصاف والصدق والتعاون:** ترتبط كل **هذه الصفات** بالمرونة، ويشمل ذلك إظهار الرعاية والاهتمام بمن يحتاجون إلى الدعم وقبول اختلافات بين الأشخاص والمودة في التعامل وعدم إساءة معاملة الغير أو التنمر عليهم وتحمل مسؤولية الأفعال، وإذا أظهر الطلاب هذه المواقف والسلوكيات تجاه الغير فمن المرجح أن يحصلوا على رد فعل إيجابي في المقابل، وهذا يساعد الطالب على الشعور بالرضا عن نفسه.

5-5-4 المهارات الاجتماعية للمرونة

تمثل المهارات الاجتماعية حجر أساس آخر من أجل تحقيق المرونة، وتشمل مهارات تكوين الصداقات والحفاظ عليها وحل الخلافات والعمل والتعاون بصورة جيدة في فرق أو مجموعات، وعندما يكون لدى الطلاب علاقات جيدة في المدرسة

والقدرة على المشاركة في الفئات المجتمعية أو الفرق الرياضية أو الأنشطة الفنية يكون لديهم فرصًا أكبر لتطوير العلاقات والشعور بالانتماء، وتعني هذه الروابط الاجتماعية أيضًا أنه قد يكون لدى الطالب علاقات مع عدد كبير من الأشخاص جديرين بالثقة يتحدث معهم عن مخاوفه أو أمور مزعجة تواجهه.

5-5-5 عادات التفكير الإيجابي لتحقيق المرونة

تتعلق المرونة بالواقعية والتفكير بعقلانية والنظر إلى الجانب المشرق وإيجاد الإيجابيات والتوقع بأن تسير الأمور بصورة جيدة والمضي قدمًا حتى عندما تبدو الأمور سيئة، فعندما يغضب أحد الطلاب أو ينزعج يمكن للمعلم أن يساعده في وضع الأمور في نصابها الصحيح من خلال التركيز على الحقائق والواقع، وفيما يلي بعض الأمثلة التي يمكن للمعلم اتباعها:

- حاول طرح سؤال "هل هذا الأمر هام حقًا بقدر ما تعتقد؟ وعلى مقياس من 1 إلى 0 ما مدى سوء هذا الأمر فعليا؟" ويمكن للمعلم أيضًا مساعدة الطالب على فهم أن حدوث أي أمر سيء في جزء من حياته لا يعني أن كل الأمور أصبحت سيئة..
- عندما يحصل الطالب على نتائج سيئة في الامتحان يمكن للمعلم أن يشير إلى أن ذلك لن يمنعه من ممارسة رياضته المفضلة في نهاية الأسبوع أو الخروج مع الأصدقاء، وعندما يكون الطالب قاسيًّا على نفسه يمكن تشجيعه بكلمات تعزز من ثقته في نفسه.
- قد يقول الطالب "سأشعر بالإحراج الشديد إذا تحدث أمام زملائي"، يمكن للمعلم أن يقترح بدائل مثل "التحدث أمام الجمهور من الأمور غير المفضلة بالنسبة لي أيضًا، ولكن بإمكاني التعايش معه" أو "ليس لدي القدرة على التحدث أمام الجمهور، ولكن من الجيد تجربة أشياء جديدة"، فمن المرجح أن يشعر الطالب بإيجابية إذا كان قادرًا على إدراك أن الأوقات الصعبة هي جزء من الحياة وأن الأمور ستتحسن بعدها، وقد يستغرق هذا الأمر وقتًا أطول مما يعتقده الطالب، لذا يمكن للمعلم مساعدة الطالب في ذلك الأمر من خلال التحدث إليه عن كيفية اجتيازه هو أو غيره لمثل هذه الأوقات العصيبة، كما يمكن للطالب إنجاز أمور من خلال هذه المهارات:
- الشعور بالثقة والقدرة على الإنجاز يُعد بمثابة جزء لا يتجزأ من المرونة.
- إن تحديد الأهداف والتخطيط والتنظيم والانضباط الذاتي والاستعداد للعمل بجد وسعة الحيلة من أهم المهارات في هذا المجال،

فيمكن للمعلم تعزيز هذه المهارات لدى طلابه من خلال مساعدتهم على تحديد نقاط قوتهم وضعفهم، ثم تشجيعه على تحديد الأهداف التي تلائم نقاط قوته، والتي تساعده على التركيز على الأمور البارع فيها، كما أن حث الطلاب على تحمل مسؤوليات جديدة أو إضافية يُعد بمثابة طريقة رائعة لبناء ثقتهم بأنفسهم، وإدراك ما يمكنهم القيام به, ومن الأمثلة على ذلك القيام بالأدوار القيادية في المدرسة أو العمل بنظام الدوام الجزئي، ومن ناحية أخرى يجب التركيز على جهد الطالب، وليس على النتائج فقط.



6-5-5 كيفية بناء المرونة الرقمية

يجب أن تركز جهود تطوير المرونة الرقمية لدى الطالب على القدرة الحاسمة والكفاءة التقنية ليصبح عنصرا فعالا لحماية نفسه والحفاظ على سلامته:

- ✓ يهدف بناء المرونة الرقمية إلى تعزيز قدرة الطالب على تحديد المخاطر الإلكترونية وشرح تأثيرها وانعكاساتها بصورة صحيحة وتنمية القدرات الفنية والعاطفية من أجل التصدي لها.
- ✓ يتطلب ذلك بناء معرفة الطلاب ووعيهم حول النطاق الكامل للمخاطر الإلكترونية دون التركيز بدرجة خاصة على مخاطر معينة أو مباشرة.
- ✓ عندما يشعر الطلاب بأنهم قادرون على التصدي للمخاطر يكونون أقل عرضة للخوف أو القلق بشأنها، ومن خلال مساعدة الطلاب على أن يصبحوا مستخدمين إلكترونيين أكثر ثقة وكفاءة -بما في ذلك القدرة على مواجهة المخاطر على الإنترنت والتعامل معها- يكون لهم القدرة على اقتناص المزيد من الفرص عبر الإنترنت دون الحاجة إلى التقيد باستراتيجيات محددة لحل المشكلات.

يجب أن تعتمد محاولات بناء المرونة الرقمية للطالب على اتباع نهج مرتكز على الطالب من خلال:

- ✓ رفع مستوى المهارات
- ✓ التشجيع على زيادة الوعي بعواقب بعض الأنشطة.
- ✓ يقوم المعلمون وصانعو السياسات بإعطاء مصداقية لخبرات الطلاب عبر الإنترنت والمخاطر والفرص المتاحة ليتسنى لهم استخدام الاستراتيجيات المستقبلية في إنشاء أطر حماية ترتبط ارتباطًا وثيقًا بتجاربهم الحياتية.

تعمل هذه التوجيهات على خلق المرونة وتقليل المخاطر للحد من الأضرار:

1- **تدابير التخفيف من حدة المخاطر:** قد يساعد ذلك على تقليل احتمالية تعرض الطالب لمحتوى ضار عبر الانترنت، ومن ذلك استخدام بطاقة تعريف المحتوى الآمن التي تجعل من السهل على الأطفال والآباء تحديد المواد المناسبة للعمر والملائمة للطفل، إضافة إلى إنشاء محتوى عالي الجودة يروق للأطفال والشباب.

2- **الشروط الأساسية للحد من المخاطر:** من ذلك التشريعات، وتحديد وحظر بعض المحتويات عبر الإنترنت كالمواد التي تتضمن الاعتداء على الأطفال، والحد من خطر تعرض الشباب لمثل هذه المواد من خلال المقاضاة الفعالة لمرتكبي جرائم مثل الاستمالة الإلكترونية.

3- **الرصد والإشراف:** يجب مراقبة الأنشطة الإلكترونية ووضع حدود الحدود لها.

4- **لاشك أن التقنية أصبحت تلعب دورًا هامًا:** إضافة إلى برنامج مكافحة الفيروسات يمكن للمعلمين تثبيت برامج من شأنها تصفية بعض مواقع الويب من عمليات البحث وحظر عرض تطبيقات أو موقع ويب أو محتوى معين. **البرامج**

5- **زيادة الوعي:** من الأمور الهامة هنا زيادة الوعي عن المخاطر المحتملة بين الطلاب وأولياء أمورهم.

القسم 6: مبادرات حماية الطلاب عبر الإنترنت

6-1 خصوصية الطلاب والإشراف عليهم والثقة بهم

6-1-1 الأمور التي يتعين على المعلمين معرفتها حول خصوصية الطالب وأسراره والإشراف عليه

1- **الخصوصية**: كلما تقدم الطالب في السن فإنه يحتاج إلى مزيد من الخصوصية والمساحة الشخصية والنفسية، وذلك لأن الطالب يواجه تحديات كبيرة في سن المراهقة مثل معرفة شخصيته وطباعه، ويكتسب الطالب أيضًا مهارات بدنية وفكرية جديدة، وينمي اهتمامات اجتماعية جديدة، فتعلم كيفية مواجهة هذه التحديات بطريقة مسؤولة ومستقلة يمثل جزءًا من النضوج.

2- **السرية**: لا تُعني الرغبة في الحصول على مزيد من الخصوصية أو قضاء بعض الوقت على إنفراد بالضرورة أن الطالب لديه ما يخفيه، حيث تتوافق السرية مع الرغبة في الاستقلال - كما أنها جزءًا طبيعيًا من فترة المراهقة، ومع ذلك قد تكون السرية الشديدة -في بعض الأحيان- بمثابة إشارة تحذير، فإذا كان الطالب يقضي ساعات طويلة في غرفته، ولم يعد يرغب في التحدث أو يبدو منطويًا حتى عندما تحاول التواصل معه فقد يكون ذلك علامة تحذير من الاكتئاب أو القلق أو التدخين أو إدمان المخدرات أو غيرها من المشاكل المشابهة، ويمكن أيضًا أن يقضي الطالب وقتًا طويلاً بمفرده على الكمبيوتر أو الإنترنت.

3- **الإشراف:** الطلاب ليسوا مستعدين دائمًا للتعامل مع البالغين، حيث أن عقولهم لا تزال في طور التطور، وهذا يعني أن الطلاب يتخذون أحيانًا قرارات سريعة، ولا يفكرون دائمًا في عواقبها أو عواقب سلوكياتهم، وقد يعرضهم ذلك للخطر، لذا لا يزال الطلاب بحاجة إلى نصيحتك ودعمك، كما أنهم بحاجة لأن يكون المعلم على تواصل معهم ومعرفة بما يخططون له - وذلك ما يُطلق عليه الإشراف، ونظرًا لأن الطلاب بحاجة أيضًا إلى الخصوصية والاستقلالية فالمعلم بحاجة إلى الإشراف عليهم بطريقة مختلفة عما كانوا عليه عندما كانوا أصغر سنًا، حيث يجب إبداء مزيد من التفهم وحسن التقدير لظروفهم، كما يجب أن يتغير أسلوب الإشراف عليهم كلما تقدموا في العمر.

6-1-2 الإشراف الجيد على الطلاب

يكون الإشراف مثاليًا عندما يكون محدودًا وغير تطفلي، ويعتمد على الثقة والبقاء على تواصل مع الطالب، فمن خلال استمرار الاتصالات والتواصل اليومي قد يميل الطالب إلى طرح ما يحدث معه وما يعيشه من مستجدات.

- ✓ عندما يعود الطالب من المدرسة إلى المنزل اطلب منه أن يخبرك بأنه وصل إلى المنزل بأمان، فهذا طلب معقول.
- ✓ ضع بعض القواعد الأساسية حول ما يمكن للطالب القيام به في وقت فراغه، وهذا يعني أن ولي الأمر لن يكون قلقا على الطالب طوال الوقت.

- ✓ واعلم ما يقرأه الطالب، وما يشاهده على التلفزيون، وما يفعله على الكمبيوتر أو الإنترنت.
- ✓ حدد بعض التوقعات حول ما تحتاج إلى معرفته من الطلاب في السنوات الأولى من المراهقة، فمن المرجح أن يقوم الطلاب بتنفيذ هذه التوقعات كلما تقدموا في السن، فعلى سبيل المثال قد يقبلوا بأنك بحاجة إلى معرفة ما يقومون به إذا كانوا معتادين على مشاركة هذه المعلومات معك منذ أن كانوا صغار.
- ✓ عندما يبدأ الطالب بالحديث معك توقف عن كل ما تفعله وأنصت إليه جيدًا، فهذا يبعث برسالة له مفادها أنك مهتم بمعرفة ما يجري في حياته.
- ✓ حاول أن تكون على دراية بما يفعله الطالب وكيف يتصرف، فقد يسهل ذلك اكتشاف أي تغييرات في سلوكه قد تشير إلى وجود مشكلة.
- ✓ راقب بشكل عام مدى التقدم الدراسي وأداء الواجبات المنزلية والمواعيد النهائية بدون الدخول في تفاصيل، وذلك الأمر يسهل تحقيقه عندما تكون هناك علاقة جيدة بين الطالب والمدرس.
- ✓ تعرف على أصدقاء الطالب، وامنحهم مساحة حركة شخصية كافية في أوقات فراغهم، فهذا يساعدك على البقاء على اتصال بأصدقاء الطالب ومعارفه دون الحاجة دائمًا إلى السؤال، كما يمكن أن يساعد التواصل مع أولياء أمور أصدقاء الطالب أيضًا في تتبع الطلاب وأصدقائهم.
- ✓ حاول تجنب جعل الطالب يفقد ثقته بك أو يشعر بأنك تقتحم خصوصيته، ولكن قد تكون هناك أوقات يحتاج فيها المراهق إلى توجيه أسئلة له بصورة حازمة للحصول على إجابات.

3-1-6 ما هو موجبات الإشراف بالنسبة للمعلم

الإشراف على الطلاب يستحق كل الجهد المبذول، حيث إن الطلاب الذين يتم الإشراف عليهم جيدًا:

- ✓ يكونون أقل عرضة للانخراط في السلوك المعادي للمجتمع - كالسرقة أو العنف.
- ✓ يكونون أقل عرضة لشرب الخمر أو تعاطي المخدرات.
- ✓ يبدأون في ممارسة الجنس في وقت متأخر، وكذلك ممارسة الجنس الآمن أكثر عندما ينشطوا جنسيًا.
- ✓ يكونون أقل عرضة للاكتئاب.
- ✓ يكون لديهم احترام الذات بدرجة كبيرة.
- ✓ يحققون نتائج دراسية أفضل، وكذلك تكون معدلات الغياب من المدرسة والحرمان المؤقت من الدراسة أقل من غيرهم.
- ✓ يستطيعون تجاوز الأوقات الصعبة.

6-1-4 تجنب استخدام تطبيقات المراقبة

يُفضل تجنب استخدام تطبيقات المراقبة التي تتيح مراقبة نشاط الطلاب عبر الإنترنت سرًا، حيث يؤدي استخدام هذه التطبيقات إلى إرسال رسالة لهم مفادها غير جديرين بالثقة، بينما يكون من الأفضل التحدث بصراحة عن استخدامك للإنترنت وتشجيع الطلاب على القيام بالأمر نفسه، وإذا اخترت مراقبة استخدام الطالب للإنترنت أثناء اتصاله بها أو مراجعة سجل المتصفح الخاص به فمن المفيد التحدث مع الطالب أولاً، ولا تحد أدوات الاستخدام الآمن للإنترنت -كعوامل تصفية الإنترنت- بالضرورة من تعرض طلاب هذه الفئة العمرية للمخاطر الإلكترونية، فقد يشجع استخدام عوامل التصفية في المنزل بعض الطلاب على الاتصال بالإنترنت في بيئات أخرى بعيدًا عن المنزل لا توجد بها تلك المرشحات، أيضًا قد يشعر الطالب بعد قدرته على التحدث معك عن تجربة سلبية عبر الإنترنت لأنه قد يشعر بالقلق من الوقوع في مشكلة أكبر لعدم استخدام المرشح.

6-1-5 كيف يجب على المعلمين التعامل مع خيانة الثقة عبر الإنترنت

تساعد الثقة المتبادلة بين الطالب والمعلم في الحفاظ على أمان الطالب عبر الإنترنت، فالمحادثات الهادئة والمفتوحة حول استخدام الإنترنت قد تساعد الطالب على الشعور بأنك على يقين بأنه سيكون شخصًا مسؤولاً على الإنترنت، وعندما يشعر بالثقة فمن المرجح أن يتحدث مع معلميه حول ما يقوم به عبر الإنترنت ويبلغه بمحتوى الإنترنت وجهات الاتصال التي تثير قلقه، وقد لا يزال الطلاب يفتقدون هذه الثقة أو يسيئون استخدام إعدادات الخصوصية، وهذا يستلزم مراقبة الطالب عن كثب لفترة حتى يستعيد ثقة المعلم، وفيما يخص الخروقات الكبيرة للثقة أو المخالفات المتكررة ستحتاج إلى اتباع أساليب جديدة لإعادة بناء الثقة بمرور الوقت،

قد تحتاج إلى استخدام إستراتيجيات مثل:

- ✓ "العقاب" (حظر الأنشطة الاجتماعية لفترة من الوقت).
- ✓ سحب الامتيازات في الالصف.
- ✓ منع الطالب من ممارسة الرياضة.
- ✓ عدم منح الطالب وقت للاسمتاع.

2-6 وسائل المعلمين للمحافظة لى أمان الطلاب أثناء الاتصال بالإنترنت

1-2-6 علامات تدل على تعرض الطالب للإيذاء عبر استخدام الإنترنت

قد يتطرق الطلاب لمحتوى مسيء، أو يتعرضوا لمخاطر عندما يكونون متصلين بالإنترنت أو عند استخدامهم للوسائل الرقمية، ويحتاج المعلمون إلى مهارات ومعارف بعينها لتحديد وإدارة مخاطر سلامة الإنترنت، فقد يكون الطالب الآن مستخدمًا مستقلًا للإنترنت، ولكن عليه بناء المهارات والمعرفة اللازمة لتحديد مخاطر السلامة وإدارتها.

- ✓ إهدار الكثير من الوقت على الإنترنت.
- ✓ السرية الزائدة - لا سيما حول استخدامه للتقنيات.
- ✓ إغلاق الباب وإخفاء ما يشاهده عندما يدخل شخص ما الغرفة.
- ✓ عدم القدرة على التحدث بصراحة عن أنشطته عبر الإنترنت.
- ✓ السلوك المضطرب عند الرد على هاتفه المحمول والميل إلى إجراء المكالمة على انفراد.
- ✓ الحديث الغامض عن صديق جديد، ولكن دون توضيح أي معلومات عنه.
- ✓ قضاء المزيد من الوقت في التحدث سرًا مع أصدقاء جدد عبر الإنترنت.

2-2-6 مساعد الطلاب على تحديد وإدارة مخاطر سلامة الإنترنت

من الهام مساعدة الطالب المراهق على إدارة مخاطر سلامة الإنترنت بنفسه. وذلك يساعد الطالب على بناء المرونة الرقمية، وهي القدرة على الاستجابة والتصدي للمخاطر التي يواجهها عبر الإنترنت بصورة إيجابية. فالأمر كله يتعلق بالوثوق في الطالب ليصبح مواطنًا رقميًا مسؤولًا، ويشمل ذلك:

- ✓ أن يصبح المعلم قدوة يُحتذى بها فيما الاستخدام الصحيح للإنترنت.
- ✓ التحدث مع الطالب حول المحتوى والسلوك الإلكتروني
- ✓ تذكير الطالب بالمحافظة على الخصوصية والمعلومات الشخصية
- ✓ تعليم الطالب أنسب طرق للشراء عبر الإنترنت

إضافة إلى ذلك يمكن للمعلم استخدام مجموعة من الاستراتيجيات لمساعدة الطلاب على إدارة مخاطر الإنترنت مثل:

- ✓ وضع هذه الخطة مع الطلاب وطلب اقتراحاتهم، وقد تشمل هذه الخطة أمور مثل المناطق التي لا تستخدم فيها الأجهزة في منزلك، ومناقشة السلوك المقبول على الإنترنت، ووضع قواعد أساسية للسلامة على الإنترنت، ويمكن للمعلم تبني خطة عائلية حول استخدم الوسائل التكنولوجية ولكن يُفضل مناقشة هذه الخطة مع الطالب.
- ✓ التحدث مع الطالب حول خصائص المحتوى غير اللائق والمزعج، ناقش هذه المواضيع بطريقة لا تُصدر من خلالها أحكامًا على تصرفاته، حينئذ سيتحدث الطالب معك إذا صادف شيئًا مزعجًا على الإنترنت، أو إذا كان لديه تجربة إلكترونية سيئة.
- ✓ البقاء على تواصل مع الطالب لمعرفة ما يقوم به ومقدار الوقت الذي يقضيه على الإنترنت، وذلك سيساعد على تحديد الوقت الذي قد يواجه الطالب فيه مشكلة.
- ✓ حث الطالب على إضافتك "كصديق" له على وسائل التواصل الاجتماعي، قد يتفهم الطلاب الأصغر سناً هذا الأمر، لكن الطلاب الأكبر سنًا يفضلون عادة عدم إضافة المعلم كصديق لأنهم يفضلون الخصوصية.
- ✓ تشجيع الطالب وحثه على تصفح الإنترنت واستخدامه بأمان - وحثه بمراجعة إعدادات الخصوصية.
- ✓ معرفة كيفية تقديم شكاوى بشأن أي محتوى إلكتروني مسيء أو غير قانوني.
- ✓ إن استخدم أدوات الأمان التقنية على شبكة الإنترنت -كمرشحات الإنترنت- قد يؤدي إلى زيادة نسبة تعرض الطلاب فوق عمر 14 عامًا للمخاطر، فإذا كان الطالب يستخدم تلك المرشحات في هذا العمر فقد لا يستطيع تطوير المهارات التي يحتاج إليها لتجنب المحتوى الغير لائق والمزعج، وقد يخاطر إما عن طريق الخطأ أو عن قصد عندما يستخدم الإنترنت في بيئات لا توجد بها تلك المرشحات.
- ✓ استخدم محركات البحث الملائمة للطلاب وعدم نشر المعلومات الشخصية واستخدم البرامج والتطبيقات المناسبة.
- ✓ ضرورة أن يكون المعلمون على معرفة بالألعاب والمواقع الإلكترونية المناسبة للطلاب، حيث يمكنهم القيام بذلك من خلال مراجعة موقع Common Sense Media الإلكتروني. (https://www.commonsensemedia.org/reviews).
- ✓ استخدم الإنترنت مع الطالب وتأكد من أنك على مقربة منه وعلى دراية بما يقوم به أثناء الاتصال بالإنترنت، ويتيح ذلك للبالغ إمكانية التصرف بسرعة وبث الطمأنينة في روح الطالب إذا كان خائفًا أو منزعجًا من محتوى معروض على الإنترنت.
- ✓ تحقق من إعدادات الخصوصية وخدمات تحديد الموقع واستخدم إعدادات البحث الآمن على المتصفحات والتطبيقات ومحركات البحث، إلخ.
- ✓ إذا قدم المعلم المساعدة فيجب عليه التأكد من اتباع الطالب لقواعد الأمان على الإنترنت كمشاهدة البرامج المناسبة لعمره فقط.

3-2-6 مناقشة مضمون المحتويات الإلكترونية

تحدث بصراحة عن طرق استخدامك للوسائل الرقمية الإنترنت، وشجع الطالب على القيام بنفس الأمر، ويساعد ذلك الطلاب على الشعور بأن لديهم شخصًا يمكنهم التحدث إليه إذا واجهوا موقفًا سيئًا عبر الإنترنت، وحثهم على مناقشة الأمر معك بمطالبتهم بشرح التطبيقات والألعاب والمحتوى الذي يهتمون به، كي تفهم نوعية البرامج التي يستخدمونها، فقد تقول "تختفي المنشورات على برنامج Snapchat سرعة، ولكن يمكن تسجيل الشاشة لما قبل حينها، فهل هذا صحيحًا؟" فمن الجيد تشجيع الطلاب على تطوير شعورهم بما يحبونه وما لا يحبونه عبر الإنترنت والدفاع عن اختياراتهم عند خوض نقاش مع الأصدقاء، على سبيل المثال يمكن قول "من الرائع أنك اخترت حظر هذا المحتوى، ولم تخوض في هذا الجدال عبر الإنترنت"، كما أن التحدث مع الطلاب عن الخدع الإلكترونية والأخبار المزيفة سيساعدهم ذلك على تطوير القدرة على معرفة ما إذا كان الموقع الإلكتروني يحتوي على معلومات جيدة أم لا.



يمكن للمعلم تجربة موقع Hoax-Slayer، وهو موقع إلكتروني يساعد على كشف الغش والخدع عبر إنترنت، وكذلك اختر إعدادات الخصوصية وتحديد الموقع والسلامة المناسبة على الأجهزة أو البرامج أو الوسائل الاجتماعية التي يستخدمها الطلاب، واشرح السبب وراء ذلك، فعلى سبيل المثال قد تقول: "غالبا ما يقوم أرباب الأعمال بعمليات بحث عبر الإنترنت لمعرفة المزيد عن مقدمي طلبات العمل، لذا تأكد من أن أي منشور تقوم بنشره على الإنترنت سيكون مناسبًا لأن يراه أرباب الأعمال المستقبليين".

يجب على الطلاب توخي الحذر عند مشاركة المعلومات الشخصية، وذكّرهم بعدم إعطاء اسمهم عنوانهم أو تاريخ ميلادهم أو غيرها من معلومات هوية للأشخاص الذين لا يعرفوهم شخصيًا، من المستحسن أيضًا استرجاع نصيحة "الغريب الخطر" مع الطالب أثناء انتقاله إلى مرحلة البلوغ، وعندما يقوم مواعدة أشخاص لا يعرفهم من خلال الإنترنت، فعلى سبيل المثال قد تقول "هناك دائمًا خطر إذا ذهبت لمقابلة شخص تعرفت عليه عبر الإنترنت، فقد يقودك ذلك إلى وضع خطير، حيث قد يرغب الشخص الذي تعرفت عليه عبر الإنترنت في إيذائك، لذا لا تثق أبدًا بأي شخص تعرفت عليه عبر الإنترنت."

4-2-6 يجب أن يكون المعلم على دراية بالمشاكل التالية للحفاظ على سلامة الطالب عبر الإنترنت

1- منع الجريمة الإلكترونية: قد تعتقد أن الطالب صغير للغاية على أن يكون ضحية للجرائم السيبرانية، ولكن كما أشارت شركة حماية سرقة الهوية Lifeloock إن هذا بالضبط ما يريده الأشرار منك أن تعتقده، ففي بعض الأحيان يستهدف سارقو الهوية المراهقات والمراهقين ممن لا يستخدموا أرقام السلامة الاجتماعية واستخدام معلوماتهم الشخصية للقيام بكافة الأمور من فتح حساب بطاقة الائتمان لشراء سيارة أو منزل، ولمنع حدوث ذلك اشرح للطالب أهمية الحفاظ على خصوصية بياناته -قدر الإمكان- عند الاتصال بالإنترنت، واشرح له أنه إذا طلب موقع من مواقع التواصل الاجتماعي أو لعبة إلكترونية بيانات كاسمه أو عنوانه أو أي نوع آخر من البيانات الشخصية فعليه إبلاغ شخص بالغ على الفور، كما يعد شراء برنامج لحماية الهوية أيضًا أمرا مستحسنا. فإذا كان لديك واحد بالفعل فحث الطالب على استخدامه، أو احصل على واحد لجميع أفراد الأسرة، يمكن الحصول على معلومات الطالب الشخصية وسرقة هوياته، أو قد يصبح ضحية للجرائم السيبرانية، وإليك بعض التوصيات لحفاظ الطالب على سلامته الشخصية على الإنترنت:

- ✓ التأكد من أن الطالب يرسل فقط معلومات بطاقة الائتمان من خلال مواقع آمنة، حيث تكتشف العديد من برامج مكافحة الفيروسات المواقع غير الآمنة، وتحذره منها.
- ✓ التفكير قبل المشاركة، حيث يجب أن يكون لدى المعلمين وأولياء الأمور بعض التوجيهات الواضحة فيما يتعلق بما يمكن للطلاب مشاركته وما لا يمكنهم مشاركته.
- ✓ التنمر هو مسألة أخرى يجب مراعاتها فيما يتعلق بمشاركة الصور، حيث يجب أن يدرك الطالب أنه يمكن لأي شخص التقاط الصورة التي نشرها للتو واستخدامها للتسلية أو التشهير به.
- ✓ تذكير الطالب بأن الأشخاص الموجودين على الجانب الآخر من الشاشة هم أشخاص حقيقيون، حيث تخلق شبكات التواصل الاجتماعي مسافة معينة بين الأشخاص، وذلك يجعل التواصل أمرًا سهلاً في بعض الأحيان.
- ✓ تحذير الطالب بشدة من المتصيدين الجنسيين على الإنترنت، وعلى المعلم التأكد من أن الطالب لن يقوم أبدًا بترتيب لقاء بينه وبين شخص ما التقى به عبر الإنترنت.
- ✓ لعب الألعاب عبر الإنترنت يخلق "ثغرة" للمخترقين؛ وذلك نظرًا لأنه يلزم تفعيل برامج ActiveX أو JavaScript لتشغيل الألعاب، وعليه يجب إغلاق هذه البرامج بعد اللعب، وإلا فإنها ستكون بمثابة ثغرة للمخترقين يتسللون من خلالها.
- ✓ أحد أبسط الأشياء التي يمكنك القيام بها هو امتلاك الكمبيوتر في منطقة "عامة" أو مفتوحة. قم بإعداده بحيث يمكنك مراقبة أي تصفح إنترنت. وبالطبع لدى العديد من المراهقين هواتف وأجهزة كمبيوتر محمولة؛ لذا لا يزال الوعي بالسلامة أمرًا بالغ الأهمية.

2- **تجنب التنمر على الإنترنت:** يمثل التنمر على الإنترنت -كما هو مبين- أحد أكثر التهديدات الشائعة التي يجب على الطالب التصدي لها عند استخدامه الكمبيوتر، فغالبًا ما ينتهي المطاف بالطلاب ممَن يتعرضون للتنمر إلى الشعور بالاكتئاب والعزلة، ولحسن الحظ توجد تطبيقات بريد إلكتروني مثل **Block Sender** تقوم بحظر الرسائل غير المرغوب فيها الواردة من بعض الأشخاص ممَن لا ترغب في أن يتواصلوا من الطالب على الإنترنت، كما يمكن إعداد التطبيق لحظر أي بريد يحتوي على كلمة أو موضوع معين، إضافة إلى ذلك تسمح العديد من تطبيقات المراسلة الفورية والدردشة للمستخدمين "بتجاهل" عناوين IP وأسماء مستخدمين معينين، وقد يكون ذلك فعالًا لأنه في كثير من الحالات إذا لم يتلق المتنمر أي رد من جانب الضحية ينتقل للبحث عن ضحية أخرى.

3- **منع التنزيل غير المقصود للفيروسات:** قد يكون الطلاب ساذجين بعض الشئ في بعض الأوقات، وغالبًا ما يعتقدون أنهم يحصلون بالفعل على لعبة فيديو مجانية بمجرد النقر على رابط معين أو الدخول في مسابقة مع جائزة. ذكر متصفحي الإنترنت من الطلاب بمقولة "إذا كان الأمر يبدو جيدًا ليكون صحيحًا، فمن المحتمل أن يكون صحيحًا" وقم بوضع قاعدة بعدم السماح لأحد بالنقر فوق أي إعلان دون إذن منك. واشرح كيف يمكن أن يؤدي ذلك إلى إصابة الكمبيوتر بالفيروسات والبرامج الضارة، مما قد يجعله عديم الفائدة، ونأمل أن تساعدهم كلماتك بأن أفعالهم قد تؤدي إلى تعطيل كافة أجهزة الكمبيوتر الموجودة بالمنزل في مقاومة رغبتهم بالنقر!

4- **استمر في السيطرة على الأمر:** الإنترنت هو مصدر مذهل للمعلومات والمرح، ولكن له أيضًا جانب مظلم، فلمنع المراهقين الفضوليين من الدخول على المواقع الإلكترونية المشكوك فيها يقترح دليل "تصفح الطالب الآمن" إبقاء الكمبيوتر في منطقة يتردد عليها أفراد المنزل بكثرة، وكذلك يُنصح باستخدام مرشحات الإنترنت والإشراف العائلي للتأكد من عدم زيارة الطالب للمواقع غير المرغوب فيها، ثم ضع اتفاقية لقواعد استخدام الإنترنت توضح ما هو مناسب وما هو غير مناسب، واحصل على موافقة الطالب عليها.

3-6 شرح السلوك الآمن والمسؤول على الإنترنت

1-3-6 شرح طرق التعرف على مخاطر السلامة على الإنترنت وإدارتها للطالب

لن تكون دائمًا على مقربة للإشراف على الطلاب عندما يكونون متصلين بالإنترنت؛ لذا من الهام تعليمهم كيفية إدارة مخاطر السلامة على الإنترنت بأنفسهم، ويساعدهم ذلك على خلق المرونة، وهي القدرة على الاستجابة للمخاطر التي يواجهونها على الإنترنت والتصدي لها صورة إيجابية، واشرح للطلاب قواعد SMART، التي تذكرهم بأن يكونوا SMART على الإنترنت،

ويجب على المعلمين استعراض هذه النصائح مع الطلاب:

- ✓ **السلامة:** حافظ على سلامتك من خلال الحرص على عدم تقديم أي معلومات شخصية كاسمك أو البريد الإلكتروني أو رقم الهاتف أو عنوان المنزل أو اسم المدرسة ولا سيما للأشخاص الذين لا تعرفهم على الإنترنت.
- ✓ **المقابلات:** قد تشكل مقابلة شخص ما تكون على تواصل معه عبر الإنترنت أمرًا خطيرًا، لذا لا تقم بذلك إلا بعد الحصول على إذن من والديك وعند وجودهم.
- ✓ **القبول:** قد يكون قبول رسائل البريد الإلكتروني أو رسائل الدردشة أو فتح ملفات مرسلة من أشخاص لا تعرفهم أو تثق بهم أمرًا خطيرًا - فقد يحتوي ذلك على فيروسات أو رسائل سيئة.
- ✓ **المعلومات الموثوقة:** قد يكذب أحد الأشخاص على الإنترنت حول شخصهم، وقد لا تكون المعلومات التي تجدها على الإنترنت موثوق بها.
- ✓ **الإبلاغ:** أخبر والديك أو معلميك أو إدارة المدرسة إذا شعرت بعدم الارتياح أو القلق من شخص أو أمر ما.

يمكن للمعلمين أيضًا القيام بذلك عن طريق:

- ✓ أن يكونوا قدوة يُحتذى بها في الاستخدام الآمن للإنترنت.
- ✓ التحدث مع الطالب حول السمعة المحتوى الإلكتروني.
- ✓ توجيه الطالب إلى الطريقة التي يجب بها مشاركة المعلومات على الإنترنت.
- ✓ تعليم الطالب أنسب طرق للشراء عبر الإنترنت

السلامة هي مساعدة الطالب على أن يصبح مواطنًا مسؤولًا عند استخدام الأجهزة الرقمية.

2-3-6 التواصل مع الطلاب عبر الإنترنت

يتيح التواصل مع الطلاب عبر الإنترنت للمعلم فرصة لمشاهدة التطبيقات أو الألعاب التي يلعبها الطلاب أو مقاطع الفيديو التي يشاهدونها، ويمكن أن يشارك المعلم في تجربة الطالب مع التحقق أيضًا من ملائمة المحتوى، وإحدى الطرق للقيام بذلك هي طرح الأسئلة التي تظهر الاهتمام بما يقوم به الطالب - على سبيل المثال "تبدو هذه اللعبة مثيرة للاهتمام، فهل يمكنك أن تعلمني كيف العبها؟"

يمكنك أيضًا عرض المواقع الممتعة أو الشيقة أو التعليمية على الطلاب، وكذلك شرح كيفية وضع الإشارة المرجعية على هذه المواقع لاستخدامها لاحقًا، وساعد الطلاب في العثور على المعلومات التي يحتاجونها للواجب المنزلي باستخدام النوع

الصحيح من الكلمات في البحث، فعندما تصادف الإعلانات المنبثقة عندما تكون متصلاً بالإنترنت فإن هذه فرصة جيدة للتحدث معهم حول عدم النقر فوقها، ويمكن للمعلمين شرح أن الإعلانات المنبثقة تؤدي إلى مواقع تحتوي على صور أو مواقع مزعجة تريد معلوماتك الشخصية أو المالية.

3-3-6 التحدث عن استخدام الإنترنت والمحتوى الإلكتروني

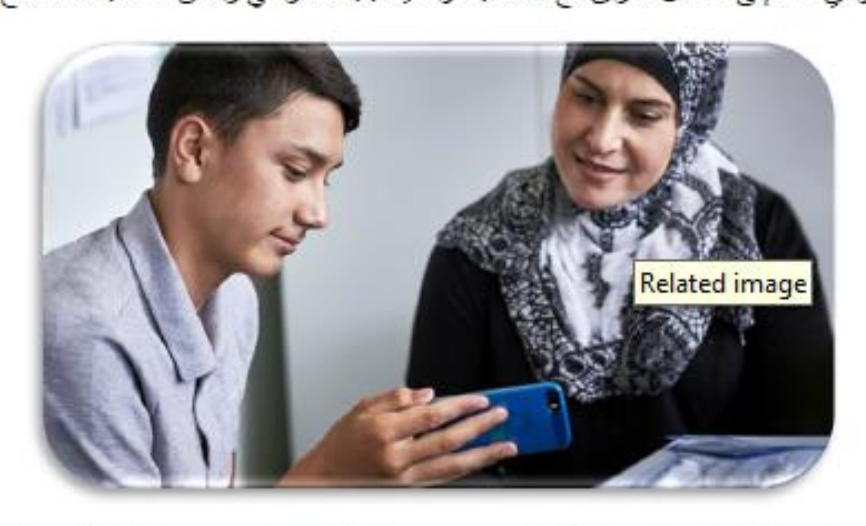
1- قبل مشاركة هذا مع الطلاب، ضع في اعتبارك راحتك، وبضعة أسباب من شأنها أن تدعو إلى إجراء محادثة حول السلامة عبر الإنترنت مع الطلاب الموضحة أدناه:

- ✓ **قد لا يعرف الغير سن الطالب:** فإذا كانوا مبتدئين في استخدام الإنترنت فقد يكونوا غير مدركين للمخاطر الكامنة في العديد من المواقع الإلكترونية الشائعة، ومن ذلك غرف الدردشة على الإنترنت ومواقع الشبكات الاجتماعية. إذا بدأ الطالب للتو في استخدام الإنترنت للبحث في المشروعات المدرسية، فتأكد من مناقشة عنصر الأمان في الإنترنت معه، ذلك لأنه لم يمر الكثير من الوقت ليكون مؤهلا لبدء التواصل مع أصدقاء جدد عبر الإنترنت.
- ✓ **مسؤولية الوالد:** أهم سبب يحتم عليك التحدث مع الطالب حول استخدام الإنترنت وأمنه هو أنه من صميم مهامك كشخص بالغ أو والد أو معلم أن توجه الطلاب وتضع حمايتهم نصب عينيك، ويجب على المعلمين وضع قواعد وتوجيهات مع طلابهم لاستخدام الإنترنت، ولا يتعين على المعلم حظر لوحات الرسائل على الإنترنت أو مواقع الشبكات الاجتماعية على الإطلاق، ولكن يجب التأكد من وضع قواعد واضحة لها يفهمها الطلاب.
- ✓ **المساعدة في الحفاظ على أمان الطلاب: بقدر** ما نود جميعًا أن تسود العالم روح الود والإحساس بالسعادة فإن الأمر ليس كذلك، ولسوء الحظ يجد الكثير من متصيدي الإيقاع بالطلاب أنه من السهل استهداف هذه الشريحة من الطلاب الصغار عبر الإنترنت، لماذا؟ لأنه يمكّن لأي شخص إنشاء هويته الخاصة على الإنترنت، ومعظم مستخدمي الإنترنت صادقون، ولكن يوجد بين هؤلاء من يرغب في أذي الغير، وعندما تتحدث إلى الطلاب حول مخاطر الإنترنت فأنت بلا شك تساعدهم في المحافظة على أمنهم وسلامتهم.
- ✓ **تعليم الطلاب ما يجب القيام به:** أما بالنسبة لتعليم الطالب ما يجب القيام به عبر الإنترنت فهناك عدد من الجوانب المختلفة التي يجب دراستها، فبالنسبة للمبتدئين علمهم كيفية استخدام الإنترنت بشكل صحيح، وخاصةً غرف الدردشة ومواقع التواصل الاجتماعي، ودعهم يعرفون أنه لا يمكنهم مناقشة المعلومات الشخصية أو مشاركة الصور أو مقاطع الفيديو مع الغرباء، وأخبرهم بما يجب عليهم فعله إذا تم استهدافهم أو مضايقتهم من قِبل شخص ما عبر الإنترنت، ومن ذلك القدوم إليك فورًا، أو حفظ جميع المعلومات بدلاً من مسحها من جهاز الكمبيوتر؛ كي تتمكن الشرطة أو أي شخص بالغ من فحصها.

- **شعور الطلاب بالراحة أكثر عند التحدث إلى شخص بالغ:** إذا كان الطلاب في مدرسة ثانوية أو إعدادية فسيتخذون وضعًا دفاعيًّا تلقائيًّا عندما تتحدث إليهم بخصوص الاستخدام الآمن للإنترنت؛ وذلك لأن معظم الطلاب يعتقدون أنهم يعرفون بالفعل كل ما يحتاجون إلى معرفته، والبعض الآخر يحس بالاستبداد من حديثك، على الرغم من ذلك فإن مناقشة الاستخدام الآمن للإنترنت مع الطلاب بطريقة هادئة وممتعة قد تجعلهم يشعرون بالراحة حيال هذه المشكلة، وهذا يقربك منهم أكثر عندما يواجهون مشاكل على الإنترنت، وعلى الرغم من أن هذا القسم يركز على مناقشة الاستخدام الآمن للإنترنت مع الطلاب فيجب تذكر أنه يجب البدء بهذا الدرس لأن المشكلة قد تظهر بمجرد تشغيل الطالب لجهاز كمبيوتر.

2- **اختيار الوقت المناسب:**

- احرص على اختيار الوقت المناسب للتحدث عن الاستخدام الآمن للإنترنت، ثم ناقش الموضوع مع الطالب مباشرةً، ولا تعلو بصوتك فيما يتعلق باستخدام المراهق للإنترنت والمخاطر بعد وقوع خلافات معه أو عندما تتصاعد وتيرة النقاش، فقد يؤدي ذلك إلى مشاكل أخرى مع الطلاب، وقد يتسبب الأمر في رفض الطالب للاستماع لمجرد تحديك.



- وفي الوقت المناسب لمناقشة الاستخدام الآمن للإنترنت مع الطالب -انتظر حتى يكون بعيدًا عن الكمبيوتر- واسأله عما إذا كان يعرف أي شيء عن الاستخدام الآمن للإنترنت والمخاطر التي تنطوي عليها هذه الشبكة، وهذه افتتاحية رائعة بمجرد أن ينهي الطالب استخدامه للكمبيوتر، وعدم الالتزام بهذا المبدأ قد يضعك في صورة الوالد المتسلط والمستبد، وذلك على الأقل في نظر الطالب.
- عند مناقشة الاستخدام الآمن للإنترنت مع الطالب من المهم عدم افتراض إلمام الطالب بالفعل بكافة أبعاد الموضوع، فإن قاطعك الطالب، وقال إنه يعرف بالفعل كيف يستخدم الإنترنت بشكل آمن، فلا تتوقف، واحرص على إعادة تأكيد وجهة نظرك، وطرح أي قواعد ترغب في أن يتبعها الطالب، وتذكر أن معظم الطلاب يعتقدون أنهم يعرفون كل شيء، لكن الكثيرين على عكس ذلك، فمثلا قد يعلم الطلاب أن هناك متصيدين على الإنترنت، ولكن هل يعلمون أيضًا أن صورهم وهم يدخنون دون السن القانونية قد يعرضهم للفصل من المدرسة أو مسائلتهم قانونيا، بغض النظر عن مدى روعة مظهرهم على صفحة MySpace؟

3- **كيف يتحدث المعلمون**

- ✓ اشرح للطلاب أن الإنترنت به جميع أنواع المحتوى، وأن البعض من هذا المحتوى غير مناسب للطلاب، وأشر إلى وجود عناصر تحكم الوالدين، وإعدادات التصفح الآمن وعوامل تصفية الإنترنت التي يتم وضعها على معظم الأجهزة للمساعدة في حماية الطلاب من المحتوى غير اللائق، لكن النتيجة هنا ليست بالمضمونة، فقد يصادف الطلاق أثناء التصفح محتوى غير لائق.
- ✓ شجع الطالب على التحدث مع شخص بالغ إذا رأى شيئًا يثير قلقه، فقد تقول مثلاً: "في بعض الأحيان يضع الناس أشياء فظيعة على الإنترنت، وبعض هذه الأشياء زائف وبعضها حقيقي، فإذا رأيت أي شيء يقلقك، أو يجعلك تشعر بعدم الارتياح، فلا تتردد في إبلاغي به".
- ✓ ساعد الطلاب على أن يقرروا بأنفسهم المواد غير المناسبة لهم، على سبيل المثال "إذا رأيت موقع ويب يحتوي على صور مخيفة أو غير مهذبة، أو ألفاظ مسيئة أو عبارات غضب، فأبلغني بذلك، فهذا ليس موقعًا مناسبًا للتصفح".
- ✓ وضح لهم أنه ليس كل المعلومات الموجودة على الإنترنت صحيحة أو مفيدة، على سبيل المثال تكون بعض الأخبار زائفة أو وهمية، وشجعهم على الريبة في الأمور التي يجدونها على الإنترنت للمساعدة في تنمية قدرتهم على معرفة ما إذا كان موقع الويب يحتوي على معلومات جيدة أم لا.
- ✓ تحدث بصراحة عن تجربتك مع الإنترنت واستخدامه، وشجع الطلاب على فعل الشيء نفسه، حيث يساعد ذلك الطلاب على الشعور بأن بإمكانهم التحدث إليك إذا واجهوا أمرًا غير مقبول على الإنترنت، ويعد طرح التجارب السلبية على الإنترنت مع شخص بالغ موثوق به أفضل وسيلة للطلاب لتنمية قدرتهم على التعامل مع المخاطر التي يواجهونها على الإنترنت، ومن المهم للطالب أن يعرف أن بإمكانه التحدث معك حول التجارب السيئة التي قد يعيشها على الإنترنت وألا يقع في أي مشكلة.
- ✓ شجع الطلاب على تنمية الشعور بما يحبونه، وما لا يحبونه على الإنترنت، واختيارهم لأصدقائهم بعناية، فقد تقول لهم "يبدو أن هذا الفيديو يجعلك تشعر بعدم الارتياح، فلا بأس أن تخبر أصدقاءك أنك تفضل عدم مشاهدة مقطع فيديو بهذا العنف المفرط".
- ✓ ووضح لهم أنه ليس كل المعلومات الموجودة على الإنترنت صحيحة أو مفيدة، حيث هناك بعض الأخبار الزائفة التي ليست صحيحة على الإطلاق، ومن المهم أن يفهم الطلاب أنه إذا كان هناك شيء لا يصدق فقد غير صحيح بالمرة.

4-3-6. مراعاة الخصوصية والمعلومات الشخصية

- ✓ أكد من عدم معرفة الطالب بطرق التواصل عبر الإنترنت مع أشخاص غير معروفين شخصيًا لديه، فمن المهم للطلاب أن يحذروا من مشاركة ما لديهم مع من لا يعرفونهم بشخصه، وقد تقول "يوجد على شبكة الإنترنت أشخاصا ليسوا بالصالحين، ونفضل ألا يعرف هؤلاء محل إقامتنا، فلا تفصح عن اسمك أو عنوانك أو تاريخ ميلادك لأي شخص عبر الإنترنت، وأبلغني إذا طلب منك أي شخص معلومات شخصية". قد يساعد ذلك على مقارنة السلوك على الإنترنت وخارجها، وذلك بطرح جملة مثل "إنك لا تعطي هذه المعلومات لشخص غريب عنك في محطة الحافلات مثلا، أليس كذلك؟"
- ✓ ويحتاج الطلاب أيضًا إلى توخي الحذر بشأن المعلومات التي يقومون بإدخالها على مواقع الويب، مثل مواقع الألعاب أو المسابقات، واتفق مع الطلاب على أنهم سيرجعون لك قبل ملء نماذج المسابقات أو العضوية على الإنترنت.
- ✓ ساعد الطلاب على تحديد إعدادات الخصوصية والأمان المناسبة لهم على جميع الأجهزة والبرامج ووسائل التواصل الاجتماعي المستخدمة، واشرح لهم أهمية ذلك، وهنا يجب إيلاء اهتمام خاص عندما يستخدم الطلاب الشبكات الاجتماعية داخل الألعاب.

شجع الطالب على ما يلي:

- ✓ الرجوع إلى شخص بالغ إذا كان هناك من هو غير معروف يتواصل معه على الإنترنت.
- ✓ عدم الإفصاح عن معلومات شخصية، فيمكن قول "بعض الأشخاص عبر الإنترنت زائفون وغشاشون، فلا تفصح لأي شخص عبر الإنترنت عن اسمك أو عنوانك أو رقم هاتفك أو تاريخ ميلادك".
- ✓ عدم إدخال معلومات شخصية على مواقع الألعاب أو المسابقات، واطلب منهم الرجوع إلى شخص بالغ قبل ملء أي نماذج مسابقات أو عضوي على الإنترنت.
- ✓ الرجوع إلى شخص بالغ قبل استخدام أي تطبيق جديد، فقد يوضح لك كيفية تعيين إعدادات الخصوصية للحفاظ على أمن وسلامة معلوماتك شخصية.

5-3-6 التحدث عن السلوك المناسب عبر الإنترنت

يساعد التحدث مع الطالب حول السلوك المناسب وغير المناسب عبر الإنترنت في تعليمه طرق الاستخدام الآمن للإنترنت، ويمكن للمعلمين:

- ✓ إبلاغ الطلاب بألا يفعلوا أو يقولوا أي شيء عبر الإنترنت وجهاً لوجه مع شخص ما.
- ✓ تشجيع الطلاب على التمعن جيدا قبل نشر صورهم أو تعليقاتهم.
- ✓ حث الطلاب على الابتعاد عن المناقشات التي تجرى عبر الإنترنت، فقد تقول "قد يقول الأصدقاء أشياء لا يقصدونها، لذا فمن الجيد السماح لهم بتخطي حالتهم المزاجية وعدم التحدث معهم مباشرة عبر الإنترنت إلا بعد مرور مدة طويلة".

6-3-6 الاتجاهات في الوساطة الأبوية لأنشطة الطلاب

الإستراتيجيات الأبوية

- ✓ بالنظر إلى احتمالية ومخاطر استخدام الوسائط الرقمية للطالب لابد من وجود إستراتيجيات أبوية لخلق موازنة ثابتة بين حماية الطلاب من الأضرار التي قد تأتي من الإنترنت، وفي الوقت نفسه عدم تقييد الفرص التعليمية والاجتماعية والإبداعية المكتسبة من استخدام الوسائط الرقمية، كما يجب على الآباء اللجوء إلى أساليب معينة للوساطة فيما يتعلق بالوصول إلى الإنترنت واستخدام الوسائط الرقمية، ومن ذلك إستراتيجيات الوساطة التقييدية والتمكينية، وهو ما يندرج ضمن هذه الفئات الأربع:
- ✓ الأدوات التقنية، بما في ذلك عوامل تصفية المحتوى وPIN/كلمات المرور والبحث الآمن وغيرها من أشكال الوساطة التقنية.
- ✓ التحدث دوريا مع الطالب حول إدارة المخاطر عبر الإنترنت.
- ✓ قواعد أو قيود الوصول إلى الإنترنت واستخدامه.
- ✓ الرقابة عند الاتصال بالإنترنت.

يقوم المعلمون بتكوين علاقات مهنية متمرة مع أولياء الأمور والمحافظة عليها من خلال:

- ✓ المشاركة في التواصل المفتوح.
- ✓ الإبلاغ عن تقدم مستوى الطالب وخيارات التعلم التي أمامه.
- ✓ التجاوب مع كافة الطلبات التعليمية المقبولة.

ما هو دور المعلمين تجاه أولياء أمور الطلاب؟

يتأثر الطلاب باستخدام أولياء أمورهم للحلول التقنية؛ لذا يجب أن يناقش المعلمون مع أولياء الأمور كيف ينبغي أن يكونوا قدوة في استخدام التقنية الصحية، ويقصد باستخدام التقنية الصحية هو استخدامها بطريقة متوازنة وإيجابية وممتعة، وأيضًا التأكد من أنها ليست سوى وسيلة من وسائل الاسترخاء أو الترفيه عن نفسك أو الحصول على المعلومات، وفيما يلي بعض الأفكار لاستخدام التقنية الصحية يمكن لأولياء الأمور استخدامها في إعداد نموذج جيد لأطفالهم:

- ✓ خصص بعض من وقت الفراغ التي تقضيه مع الهاتف يوميا لتقضيه مع أطفالك، ويمكن الاستفادة من هذا الوقت عندما يصل أطفالك إلى المنزل قادمين من المدرسة، أو عندما تصل إلى المنزل من العمل، وكذلك أثناء أوقات الوجبات العائلية، وعند ممارسة أطفالك للأنشطة الرياضة، إلخ.
- ✓ وعندما تصلك رسالة نصية أو رسالة تحديث لوسائل التواصل الاجتماعي أثناء التحدث إلى شخص ما -وخاصةً أطفالك- انتظر حتى تنتهي المحادثة قبل التحقق من ذلك.
- ✓ حاول ألا يكون هاتفك أو جهازك اللوحي أو الكمبيوتر المحمول في غرفة النوم ليلاً، واشحن أجهزة الوسائط ليلا في المطبخ أو غرفة الجلوس، وعلِّم أطفالك أن يقتدوا بك في ذلك.
- ✓ أغلق التلفزيون أثناء أوقات الوجبات العائلية، أو عندما يكون "قيد التشغيل في الخلفية".
- ✓ وحاول الاستماع إلى بعض الموسيقى أو البودكاست بدلاً من ذلك.
- ✓ ساعد أطفالك في إعداد خطة وسائط للعائلة، ثم احرص على اتباع الإرشادات الواردة في الخطة!
- ✓ استخدم حل تقني للبقاء على اتصال مع العائلة والأصدقاء عن طريق إرسال رسائل نصية أو إجراء مكالمات الفيديو أو استخدام وسائل التواصل الاجتماعي.

4-6 كيف يناقش المعلمون الاستخدام الآمن للإنترنت مع طلابهم؟

1-4-6 يجب تدريب المعلمين على إبقاء الطلاب في أمان عبر الإنترنت

هناك أربع علامات تبين للمعلمين أن الطالب في مشكلة على الإنترنت، فإذا كانت أي من هذه العلامات تنطبق على الطلاب فعليك اتخاذ إجراء على الفور.

1- **استخدام الكمبيوتر في نفس الوقت كل يوم**: ما لا يدركه الكثير من المعلمين أن الطلاب يمكنهم بسهولة أن يصبحوا أهدافًا لمتصيدي الطلاب على الإنترنت، ولا يدرك الكثير أن هذه العملية لا تحدث دائمًا بين عشية وضحاها، ويتظاهر بعض متصيدي الطلاب بأنهم في عمر الطلاب الذي يستهدفونهم، ومن ثم يعملون على كسب ثقتهم، وقد يستغرق ذلك بضعة أيام أو بضعة أسابيع، وقد يمكن معرفة ما إذا كان هذا الأمر يحدث مع الطالب عند استخدامه للإنترنت في نفس الوقت كل يوم، وتُعد تلك علامة جيدة على أنهم يتواصلون بشكل مباشر مع شخص سيئ النية.

2- **التكتم عند استخدامهم الكمبيوتر**: كيف يتصرف الطالب عندما يستخدم الكمبيوتر؟ هل يحاول إخفاء ما يفعله أثناء الاتصال بالإنترنت؟ إن قام بإغلاق جهاز الكمبيوتر تلقائيًا، أو قام بتشغيل لعبة على الشاشة فقد يحاول منعك من رؤية ما يقوم به على الإنترنت، وتُعد هذه علامة على أنه يفعل شيئًا ممنوعا، كإجراء محادثة شخصية مباشرة مع شخص غريب من متصيدي الطلاب.

3- **الشعور بالسعادة عند تسجيل الخروج من الكمبيوتر**: إذا ظهر على الطالب شعورا بالسعادة المفرطة عند تسجيل الخروج من الإنترنت فقد يكون في طريق تؤدي به إلى متاعب، ورغم ذلك قد تكون هذه العلامة خادعة بعض الشيء، فقد يكون الطالب سعيدًا لأنه انتهى للتو من مشروع دراسي طويل، لكنك لن تعرف ذلك بصراحة، وإذا كان الطالب على اتصال بشخص ما عبر الإنترنت فقد يكون بصدد بدء علاقة هو سعيد بها، ولسوء الحظ لا يدرك أنه يمكن لأي شخص الاختباء خلف شاشة الكمبيوتر، لذا من المهم أن تتحدث مع الطالب حول مخاطر بدء علاقة رومانسية على الإنترنت.

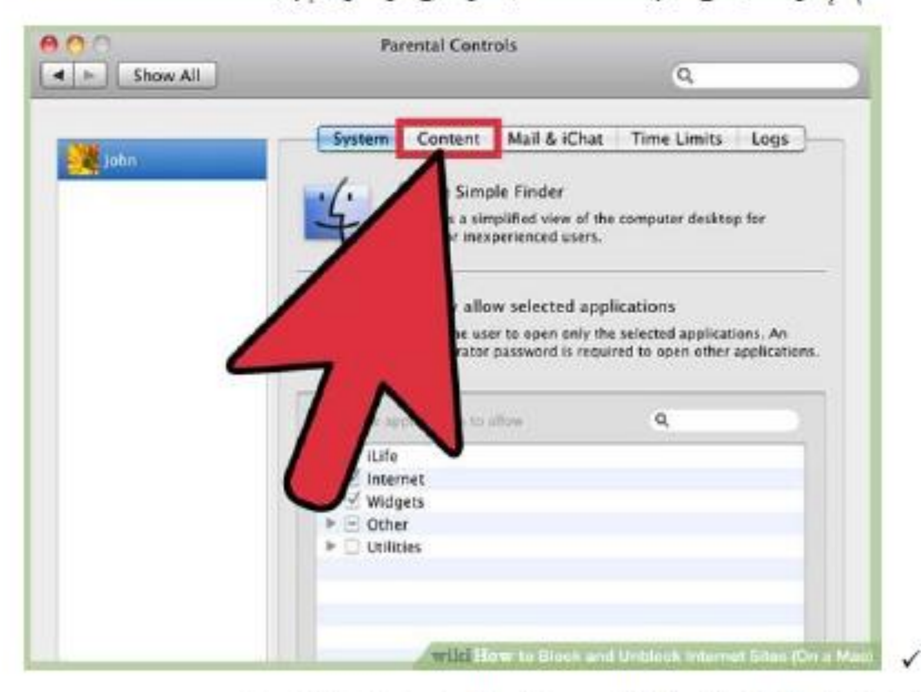
4- **شعور الطلاب بالاكتئاب**: قد يكون الطالب سعيدًا جدًا عند استخدام الإنترنت، ولكن هناك علامة تحذير أخرى وهي شعوره بالاكتئاب، خاصةً عند تسجيل الخروج من الكمبيوتر، ما لا يدركه الكثير من الآباء هو أن البعض قد يستخدم الإنترنت للمضايقة، فإذا كان لدى الطالب خلاف مع أحد أصدقائه، فقد يجد نفسه يتعرض للمضايقة عبر الإنترنت، وإذا كان هذا هو الحال فقد يبدو الطالب شديد الإحباط والاكتئاب والانسحاب.

العلامات الأربع المذكورة أعلاه ليست سوى بعض العلامات التي تريد البحث عنها لمعرفة ما إذا كان الطالب في مشكلة عبر الإنترنت أم لا، ومع ذلك هناك المزيد من العلامات يجب أن تكون على حذر منها، وأهم تلك العلامات هو حدوث تغيير في السلوك، إذا كنت تشك في مواجهة الطالب لمشكلة ما أو على وشك أن يواجه مشكلة عبر الإنترنت، فاحرص على التحدث معه في أسرع وقت ممكن.

التوصيات تساعد على ضمان خلق عادات الاستخدام الجيد للإنترنت لدى الطلاب وتأمين استخدامه له.

- ✓ **مناقشة مواضع الأخطار:** إذا كان عمر الطالب كبيرًا بما يكفي لاستخدام التقنيات والإنترنت، فهذا يعني أنه قد بلغ أيضا السن التي تؤهله للتحدث معه حول المخاطر، ولا ينبغي تخويف الطلاب، أو أن تكون صريحًا في الحديث، ولكن يجب أن تنقل للطلاب مخاطر الجرائم الإلكترونية والاستدراج عبر الإنترنت، ويهدف التواصل بصراحة حول مشكلات الإنترنت أن يتكون لدى الطلاب موقفًا صحيًّا حول استخدامه.
- ✓ **وضع الحدود:** ينطوي وضع بعض القواعد الأساسية حول استخدام الإنترنت والتقنيات على عدد من الفوائد للطالب، ففي السن المبكرة قد تتضمن الحدود قيودًا على استخدام أي وسيلة من وسائل التواصل الاجتماعي والتواصل مع الأصدقاء، ومع تقدم الطلاب في السن يجب منحهم مزيدًا من الحرية، ولكن من الأفضل تحديد المدة الذي يقضونها على الإنترنت وتقييد المواقع المناسبة للعمر التي يمكنهم الوصول إليها، كما يجب فرض قيود على السن في الألعاب.
- ✓ **وضع الرقابة الأبوية:** ساعد العصر الرقمي على توسيع العالم في نظر الطلاب، ولكن هناك بعض الأمور التي لا ينبغي السماح لهم برؤيتها، كما يمكن تعيين تربويين على شبكات النطاق العريض والشبكات المحمولة ومحركات البحث، ويمكن الاستعانة بهم لمنع الطلاب من الوصول إلى المحتوى غير المناسب لعمرهم، ومنعهم من شراء تطبيقات بعينها، وتغيير كلمات المرور وإعدادات الخصوصية.
- ✓ **استكشاف عالم الإنترنت معًا:** الإنترنت مورد مفيد من موارد التعليم، ويجب تشجيع الطلاب على استخدامه للبحث، وقد تجعل الألعاب والتطبيقات التعليمية من التعلم متعة، فقضاء بعض الوقت على الإنترنت مع الطلاب يعني أن بإمكانهم استكشاف إمكاناته بطريقة آمنة ومحكومة، ويقوم الطلاب الأصغر سنًا بتطوير مهارات تقنية المعلومات الأساسية عندما يتعرفون على كيفية استخدامك لأجهزة الكمبيوتر والأجهزة الأخرى للوصول إلى المتصفحات وحسابات البريد الإلكتروني.
- ✓ **زيادة الوعي بالتنمر على الإنترنت:** غيرت وسائل التواصل الاجتماعي والإنترنت الطريقة التي يتعرض بها الطلاب للتنمر، لكن لا يزال من الممكن أن تكون هذه الوسائل وخيمة، وقد يقع التنمر على الإنترنت من خلال البريد الإلكتروني ومنصات الألعاب والنصوص والشبكات الاجتماعية، ويتخذ هذا النمط من التنمر أشكال عديدة منها المضايقة والتهديد والترويع ونشر معلومات شخصية عن شخص آخر بشكل علني، قم بإجراء محادثات مفتوحة مع الطلاب حول التنمر عبر الإنترنت، وشجعهم على التحدث إليك إذا وقعوا ضحية له، وقد يؤدي الكشف عن المعلومات الشخصية عبر الإنترنت إلى هجمات شخصية وإلى إساءة استخدامها.
- ✓ **تسليط الضوء على مخاطر تكوين صداقات عبر الإنترنت:** يعتبر بعض الطلاب -من منطلق براءتهم- أنه من المسلم به أن من يقابلونهم عبر الإنترنت هم بالفعل كما يصفون أنفسهم، وقد تكون المنتديات وغرف الدردشة أماكن خطرة،

ويشير البحث إلى أنها تمثل مكانًا للصيد لذوي الميل الجنسي الانحرافي للأطفال ولمن يودون إيذاء الطلاب، وفي بعض الأحيان يمكن هندمة الطالب عبر الإنترنت من قبل أشخاص يضمرون بعد ذلك مقابلته سراً، ومن الجيد أن يتواصل الشباب مع أصدقاء المدرسة عبر الإنترنت، لكن حذرهم من المخاطر المحتملة لتكوين صداقات مع الغرباء في العالم الافتراضي، وتعني التطورات في العالم التقني أن الطلاب عليهم أن يعتادوا على العيش في عالم متصل، وإذا علمهم الآباء كيفية استخدام الإنترنت بأمان، فليست هناك حاجة لرفض الوصول إليه.



✓

6-4-2 الرقابة الأبوية على الإنترنت: لماذا يجب على المعلمين استخدامها

- ✓ أحد أهم أسباب وضع رقابة أبوية هو إمكانية حماية الطلاب في حالة اتصالهم بالإنترنت، وعلى الرغم من أن أدوات الرقابة الأبوية تأتي بعدد من التنسيقات المختلفة، إلا أن معظمها يسمح للشخص بحظر مواقع الويب التي لا يريد أن يشاهدها الطلاب.
- ✓ سبب آخر لوضع أدوات الرقابة الأبوية على جهاز كمبيوتر الطالب هو أنها سهلة التثبيت، كما أن معظمها ذاتي الشرح.
- ✓ إضافة إلى كون أدوات الرقابة الأبوية سهلة التثبيت فمن السهل أيضًا العثور عليها.
- ✓ لكن لسوء الحظ لا يثبت الكثير من الآباء أدوات الرقابة الأبوية؛ لأنهم يعتقدون أنها ستحد من استخدامهم الشخصي للإنترنت، ولأنك تريد أن يتجنب الطالب مواقع الويب التي تحتوي على لغة غير مهذبة أو مواضيع عنيفة فهذا لا يعني بالضرورة أنك لا ترغب في عرضها.
- ✓ لكن قبل أن تنتابك الثقة الذائفة هناك بعض الأشياء المهمة التي يجب أن تعرفها، أولاً ضع في ذهنك أن الكثير من الطلاب يتمتعون بذكاء في التعامل مع الكمبيوتر، فقد يعرف ابنك المراهق بالفعل كيف يتخطى الرقابة الأبوية، حتى لو لم يكن يعرف كلمة المرور الخاصة بك، وهذا هو السبب وراء الحاجة إلى فحص جهاز الكمبيوتر من وقت لآخر.

- ✓ وبالنسبة لضرورة تعيين كلمة مرور احرص على عدم إعطاء كلمة المرور هذه للطالب. وإذا احتاجوا إلى الوصول إلى موقع ويب تم حظره عن طريق الخطأ، مثل مشروع بحث مدرسي فينبغي إدخال كلمة المرور بنفسك لإلغاء تأمين موقع الويب حتى مؤقتًا فقط.

3-4-6 أدوات وعادات الاستخدام الآمن للإنترنت التي توفر حماية للطلاب

- ✓ الجميل في أدوات الاستخدام الآمن للإنترنت هو أنها مصممة للرقابة الأبوية والمدرسية من خلال العديد من الخيارات، وعادةً نجد أن معظم هذه الأدوات تندرج تحت عنوان الرقابة الأبوية. وتُعد القدرة على تقييم مواقع الويب وتعيين المستويات لما تريد أن يشاهده الطالب عبر الإنترنت من الخيارات المتاحة لك. ويقرر المعلم نوع المحتوى الذي يرغب أن يشاهده الطلاب. على سبيل المثال هل ترغب في إبعاد الطالب عن مواقع الإنترنت التي تستخدم لغة غير مهذبة أو عنيفة؟ إذا كان الأمر كذلك فاضبط مستوى موقع الويب لذكر ذلك صراحة، وحظر مواقع الويب تلقائيًا.
- ✓ إضافة إلى حظر مواقع الويب من خلال استخدام أدوات تصنيف المواقع يمكن أيضًا حجب مواقع الويب تمامًا. على سبيل المثال إذا كنت ترغب في حظر مواقع الشبكات الاجتماعية -مثل MySpace و Facebook- فكل ما عليك فعله هو إدخال عنوان الموقع والضغط على خيار الحجب، ويمنحك مستعرض الويب خيار السماح بقائمة مواقع الويب الموافق عليها.
- ✓ يمكن أيضًا استخدام أدوات تتبع الكلمات المفتاحية، ومع ذلك قد تواجه مشاكل في عدم الالتزام بالخصوصية، وهذا هو السبب الذي يجعل من المهم للمعلم أن يعتمد على تقدير الشخصي واتخاذ القرار كوالد، وتعمل أدوات تتبع الكلمات المفتاحية بتسجيل كل كلمة يكتبها الطالب. وفي بعض الأحيان تُعد برامج تتبع الكلمات المفتاحية وسيلة رائعة للتعرف على طلاب يتواصلون مع شخص أكبر سناً أو مع متصيد جنسي.
- ✓ هناك أيضًا أدوات للاستخدام الآمن للإنترنت تعمل على الحفاظ على سريو معلومات الطالب الشخصية، وتُعد هذه طريقة رائعة للتأكد من عدم مشاركة الطالب لأي معلومات شخصية عن نفسه مع الغرباء عبر الإنترنت.

القسم 7: دليل موارد الفصل الدراسي لإشراك الطلاب في الأمن السيبراني

7-1 موارد الفصل الدراسي والتطوير المهني

7-1-1 الأساليب التي يمكن للمعلمين استخدامها لتعريف الطلاب بمفهوم الأمن السيبراني

من نتائج إتاحة الحلول التقنية أن سهل على المعلمين استخدام طرق تفوق التعليم الإلكتروني والكتب المدرسية، ويجب استخدام الحلول التقنية المتكاملة جنبًا إلى جنب مع الأدوات المتاحة بالفعل في الفصل الدراسي؛ وذلك لتسهل على الطلاب قبول الموضوع واستيعابه، وإدراكًا لدرجات الدمج التقني يمكن للمعلمين الجدد وذوي الخبرة أن يفهموا إلى أي مدى يمكنهم الاستفادة من هذه الوسائل التعليمية الجديدة لدعم نمو أفضل للطلاب.



1- **مراحل أدوات التعلم الجديدة:** هناك أربع مراحل من أدوات التعلم الجديدة التي تستخدم الحلول التقنية لكي تستفيد منها: الإحلال والتنمية والتعديل وإعادة التعريف.

أ- **الإحلال**: في هذه المرحلة من إدماج التقنية في العملية التعليمية تعمل التقنية كبديل للأساليب السابقة اليدوية للتعليم أو التنظيم، وهذا يعني أنه بينما يتم استخدام التقنية إلا أنها لا تغير طريقة التدريس من الناحية الوظيفية.

ب- **التنمية**: تأخذ التنمية مزايا التقنية إلى أبعد من ذلك بقليل، فبدلاً من مجرد استبدال أداة تقليدية بأداة إلكترونية فهي أيضا تضمن التغييرات الوظيفية التي توفرها هذه البدائل.

ج- **التعديل**: الآن وبدلاً من مجرد إضافة ميزات أكثر للتعليم يأتي التعديل كمستوى يتم فيه إعادة تصميم مهام التدريس جزئيًا أو كليًا بناءً على الأدوات التقنية.

د- **إعادة التعريف**: إضافة إلى تعديل أساليب التدريس الحالية توفِّر الحلول التقنية فرصة لخلق طرق جديدة تمامًا للتعليم، وقد تكون هذه المهام غير مطروحة قبل الدمج التقني.

وقبل أن يبدأ المعلم في النشاط يجب عليه النظر في مفاهيم الموافقة والسرية والدعم، وينصح التربويون بمراعاة ما يلي:

- ✓ الحصول على موافقة الطلاب وأولياء الأمور.

- ✓ إعطاء الطلاب الفرصة للخروج في أي مرحلة إذا شعروا بعدم الارتياح.
- ✓ توفير معلومات حول نوع الدعم المتاح (والتأكد من توفره مسبقًا) في حالة شعور أي طالب بالقلق أو الانزعاج خلال العملية.
- ✓ التواصل الصريح حول كيفية استخدام المعلومات التي تم جمعها ومع من سيتم مشاركتها.
- ✓ ضمان أن تكون هذه الردود غير منسوبة إلى أحد (إذا كنت تستخدم استبيانا).

2- **موارد الفصل الدراسي:** قد يكون تصنيف جميع الموارد المتاحة عبر الإنترنت أمرًا صعبا، لذا جمعنا مجموعة مختارة من الموارد لدعم التخطيط أو للاستخدام مباشرة مع الطلاب، ويجب أن لدى التربوي القدرة على تصفية الموارد وفقًا للمستوى الدراسي و/أو الموضوع، اختر المستوى الدراسي: الابتدائي أو الإعدادي أو الثانوي. يمكن كمثال تصفية الموارد المتاحة حسب الموضوع:

- المواطنة الرقمية
- أمان الإنترنت
- التنمر على الانترنت
- البصمة الرقمية والسمعة

7-1- 2 وسائل حث الطلاب على الاهتمام والمشاركة في الأمن السيبراني

1- المناهج المقترحة:

- ✓ **الانضمام إلى معسكرات التدريب:** يترك للمعلم معرفة المزيد عن مثل هذه البرامج، والحصول على أكبر قدر ممكن من المعلومات حولها، ومن تم اختيار المعسكر الذي سيختار الطلاب الانضمام إليه، وتوفِّر المخيمات الصيفية أسبوع واحد من التدريب المتخصص في مجال الأمن السيبراني.
- ✓ **المشاركة في المسابقات:** الهدف الرئيسي من وراء تنظيم مثل هذه المسابقات هو توفير بيئة ممتعة ومليئة بالتحديات لتشجيع وإلهام الطلاب لاكتساب المعرفة والمهارات اللازمة للشعور بالأمان، كالمحافظة على الأجهزة الشخصية مثلا.
- ✓ **المشاركة في الرحلات.** يمكن للمدارس تنظيم رحلات داخل المكاتب الحكومية والخاصة التي تتعامل مع الأمن السيبراني.
- ✓ **الحصول على دورات تدريبية:** يمكن للمعلم تشجيع الطلاب في سن مناسب (يفضل من 10 إلى 12 سنة) على الحصول على دورات تدريبية داخلية في المؤسسات الحكومية للحصول على خبرة عملية، ويمكنهم تحقيق نجاح في العالم الحقيقي ليتعلموا كيف يؤمنون أنفسهم في العالم الافتراضي.
- ✓ **التطوع لتعليم الشباب أمورًا متعلقة بالأمن السيبراني:** يساعد هذا التطوع المعلمين كثيرا بعدم الإتقال عليهم بمهام تدريسية بل قد يكون ذلك أيضًا تجربة إيجابية للطلاب عند وضع أنفسهم مكان معلمهم، فمن يدري - قد يهتمون بالفعل بتدريس الأمن السيبراني للجيل القادم.

2- يساعد المعلمون الطلاب خلال الأنشطة بما يلي:

- ✓ **إعطائهم نموذجًا يحتذى به:** يبحث دائما الطلاب عن نماذج يحتذون بها، حتى وإن لم يكن ذلك من أهدافهم في البداية، وإذا كنت ترغب في تشجيع الأطفال والشباب على أن يكونوا خبراء في مجال بعينة فيجب على المعلم تعريفهم بالشخصيات التي يمكنهم محاكاتها.
- ✓ **تطوير مهارات الطلاب الدقيقة:** يساعد رفع مستوى المهارات الدقيقة الطلاب في مرحلة الدراسة ومرحلة ما بعد التخرج، كما يساعدهم أيضا على البقاء في وظائفهم لفترات طويلة.
- ✓ **التعرف على المواهب التي يمكن استخدامها في الأمن السيبراني:** قد يشعر بعض الطلاب بالرغبة في التأجيل أو عدم الصلاحية لمتابعة الوظائف التي يرون أنها فنية للغاية، وهناك شخصيات إبداعية لديه القدرة على التفكير خارج الصندوق عندما يتعلق الأمر بحل المشكلات والابتكار، خاصةً عندما يتم تدريبهم بشكل مناسب، ويمكن للمعلم الاستفادة من الدراسات الكامنة وراء هذه الادعاءات لإثارة اهتمام الطلاب.
- ✓ **توفير منصة للطلاب للتعلم والمشاركة وتطبيق ما تعلموه:** قد لا يكون من الصعب حاليا العثور على منصة -مثل يوتيوب- للتعلم والمشاركة والتطبيق، وهناك أيضًا GitHub للبرمجة البسيطة إذا كان طفلك يميل إلى المراسلات أكثر من مواقع التواصل الاجتماعي للاتصال بأصدقائه، وهناك أيضًا Discord حيث يمكن للزائر إنشاء غرفة وطرح الأفكار على الأعضاء الذين يمكنهم المساعدة في بلورتها والإضافة إليها.
- ✓ **التعليم من خلال ألعاب الفيديو:** قد يؤدي التعليم من خلال ألعاب الفيديو أو آليات الألعاب وتصميمها إلى تحقيق نتائج هامة في المنزل؛ مما قد يضع الطلاب في حيرة من أمرهم، ينتج عنها تحقيق مشاركة عالية في مثل هذه البيئات، وهناك بعض الطرق يمكن للمعلمين من خلالها تطبيق هذا، فبإمكانهم تغيير نظام تسمية الفصول الدراسية من التسمية بالحروف إلى التسمية "بنقاط الخبرة"، ومنح الطلاب حوافز ملموسة مثل الشارات وتنفيذ البطولات بين مجموعات صغيرة داخل الفصل واستخدام الألعاب الفعلية التي تساعد على تعلم مفاهيم معينة كالأمن السيبراني والخصوصية واختراق المواقع.
- ✓ **تعليم الطلاب المهارات الأمنية اللازمة:** لا يمكن تأهيل الفرد للعمل في مجال الأمن السيبراني أو في أي مجال آخر حتى يعرف أساسياته، وسيتعلم الطلاب أفضل أساليب الأمان وتكييفها لحماية أصولهم وأصول الشركة بمجرد تقدمهم في الدراسة وبدء العمل، ويجب أن يكون هناك ما يشبه الركيزة الأساسية أو حجر الأساس الأمني للاعتماد عليه.
- ✓ **ترسيخ أهمية التطوير المستمر في الطلاب:** يجب ألا يبدأ التعليم وينتهي في المؤسسات، فقد يبدو هذا بمثابة عدم وجود عقل، ولكن من المهم تذكير الطلاب بأنه على الرغم من حتمية تعلم الأمور المتعلقة بمختلف الوظيفة العملية إلا أنه من المهم -بنفس القدر- بذل جهد لفهم المفاهيم التي لم يتعرضوا لها في الفصل الدراسي من خلال القراءة والبحث عبر الانترنت.

✓ **توسيع جهود التعليم والتدريب في مجال الأمن السيبراني لتشمل جميع الطلاب:** يجب أن يتضمن المنهج تطبيقات عملية للأمن في حيات الطلاب المهنية، وكيف يمكن للممارسات غير الآمنة أن تهدد -ليس فقط عملهم- ولكن أيضًا العملاء الذين سيخدمونهم، تُعد سيناريوهات العالم الحقيقي والأمثلة أفضل دراسات حالات.



3-1-7 التعرف على كيفية دمج الأمن السيبراني في الفصل الدراسي

يجب أن يكون المعلم على دراية باستخدام C3 Framework لتعزيز الاستخدام المسؤول، وذلك بأن يكون ملماً بمفاهيم مثل: أخلاقيات الإنترنت والأمان السيبراني والأمن السيبراني.

1- **أخلاقيات الإنترنت:** يتعرف الطلاب ويتدربون على الاستخدام المسؤول واللائق عند الدخول على الإنترنت أو استخدامها أو التعاون مع الغير من خلالها، وعند إبداع تقنيات وأنظمة تقنية ووسائط رقمية وتقنية معلومات، كما يبدون فهمًا للمعايير الأخلاقية والقانونية المعمول بها حاليًا والحقوق والضوابط التي تحكم الأنظمة التقنية والوسائط الرقمية وتقنية المعلومات في سياق المجتمع الذي نعيشه، ويحتاجون إلى:

✓ فهم واتباع سياسات مقبولة (من لمدرسة والمنزل والمجتمع) وإدراك العواقب الشخصية والمجتمعية التي تنجم عن الاستخدام غير اللائق.

✓ عرض السلوكيات الأخلاقية والقانونية بين الأقران والأسرة والمجتمع والدفاع عنها.

✓ التدرب على ذكر مصادر المعلومات النصية والرقمية واتخاذ قرارات مستنيرة بشأن أفضل الطرق لتجنُّب السرقات الأدبية.

✓ اتخاذ قرارات أخلاقية وقانونية أثناء استخدام التقنيات والوسائط الرقمية والأنظمة التقنية عند التعرض لمشكلات في الاستخدام.

✓ التحلي بالمسؤولية وآداب التعامل على الإنترنت عند التواصل الرقمي مع الغير.

- ✔ التعرف على الدلائل والآثار النفسية والعواقب القانونية للتنمّر الإلكتروني والحلول الفعالة لمكافحته.
- ✔ التعرف على الوقت والمكان المناسب لاستخدام الأدوات والتقنيات والموارد الرقمية.
- ✔ فهم أهمية إدارة الهوية على الإنترنت ومراقبتها.
- ✔ تشجيع الغير على فهم أهمية إدارة السمعة على الإنترنت.

2- **السلامة على الإنترنت:** يتدرب الطلاب على الاستراتيجيات الآمنة لحماية أنفسهم، وتحسين مستوى التعافي المادي والنفسي عند استخدام التقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات بما في ذلك الإنترنت، ويحتاجون إلى:

- ✔ التعرف على مخاطر الشبكة بغية اتخاذ قرارات مستنيرة وإجراءات مناسبة لحماية أنفسهم حال استخدامهم للأنظمة التقنية والوسائط الرقمية وتقنية المعلومات.
- ✔ اتخاذ قرارات مستنيرة بشأن توفير الحماية المناسبة وخوض ممارسات آمنة في مختلف المواقف.
- ✔ عرض السلوكيات الآمنة على الأصدقاء وأفراد الأسرة والمجتمع وتشجيعهم عليها.

3- **الأمن السيبراني:** يتدرب الطلاب على الاستراتيجيات الآمنة عند استخدام الأنظمة التقنية والوسائط الرقمية وتقنية المعلومات، والتي من شأنها أن تضمن لهم الحماية الشخصية، وتساعدهم على الدفاع عن أمنهم على الإنترنت، ويحتاجون إلى:

- ✔ التعرف على مخاطر الإنترنت واتخاذ قرارات مستنيرة وإجراءات مناسبة لحماية أنفسهم حال استخدامهم الأنظمة التقنية والوسائط الرقمية وتقنية المعلومات.
- ✔ اتخاذ قرارات مستنيرة بشان توفير الحماية المناسبة وخوض ممارسات آمنة في مختلف المواقف.
- ✔ إظهار الالتزام بمواصلة الاطلاع على كل ما هو جديد في موضوعات الأمان والبرامج وممارسات الأمان الفعالة على الإنترنت.
- ✔ عرض الممارسات والسلوكيات الآمنة على الأصدقاء وأفراد الأسرة والمجتمع وتشجيعهم عليها.

4-1-7 تدريب الطلاب على الاستراتيجيات الآمنة في إطار السلامة والأمان وأخلاقيات الإنترنت

1- السلامة على الإنترنت

التعافي المادي والنفسي:

يتدرب الطلاب على الاستراتيجيات الآمنة لحماية أنفسهم، وتعزيز التعافي المادي والنفسي عند استخدام التقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات بما في ذلك الإنترنت، من المشكلات التي تعرض السلامة للمخاطر ما يلي: تحميل وتنزيل المحتويات غير المرغوب فيها والتنمر الإلكتروني وتشويه السمعة والرد على الرسائل غير المرغوب فيها المُرسلة من جهات أو محتالين وإدمان الإنترنت.

	K-6	9-7	13-10
أ. التعرف على مخاطر الإنترنت، واتخاذ قرارات مستنيرة وإجراءات مناسبة لحماية النفس حال استخدام التقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات.	**الممارسات الآمنة والمسؤولة** ✓ التعرف على موضوعات الأمان المتعلقة بالتقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات ومنها شبكة الإنترنت (كوسائل الاحتيال الإلكتروني ونشر المحتويات المثيرة للجدل). ✓ الميل لممارسات آمنة عند استخدام التقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات ومنها الإنترنت. ✓ معرفة وفهم الغرض من تدابير المحافظة على الأمان ذات الصلة بالتقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات.	**الممارسات الآمنة والمسؤولة** ✓ التعرف على موضوعات الأمان المرتبطة بالتقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات ومنها الإنترنت (كوسائل الاحتيال الإلكتروني ونشر المحتويات المثيرة للجدل) ومناقشتها. ✓ تبني ممارسات آمنة عند التعامل مع التقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات ومنها الإنترنت. ✓ إدراك وفهم الغرض من تدابير الحفاظ على أمان التقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات.	**الممارسات الآمنة والمسؤولة** ✓ التعرف على موضوعات الأمان المرتبطة بالتقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات ومنها الإنترنت (كوسائل الاحتيال الإلكتروني ونشر المحتويات المثيرة للجدل) ومناقشتها. ✓ تبني ممارسات آمنة عند التعامل مع التقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات ومنها الإنترنت. ✓ توضيح الهدف من استخدام مختلف مقاييس الحماية في التقنية والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات وتحليله.
ب. اتخاذ قرارات مستنيرة حول أنسب طرق الحماية والتمسك بالممارسات الآمنة في مختلف المواقف.	✓ الالتزام بتوجيهات وسياسات وإجراءات الأمان. ✓ مناقشة احتمالية ظهور السلوكيات المدمنة والاستخدام المفرط للتقنيات والإنترنت. ✓ بيان إجراءات الخروج من المواقف غير اللائقة. ✓ بيان إجراءات الحد من فرص الوقوع كضحية للتنمر عبر الإنترنت. ✓ بيان إجراءات الإبلاغ عن عمليات	✓ الالتزام بتوجيهات وسياسات وإجراءات الأمان. ✓ بيان سلوكيات إدمان استخدام التقنيات والإنترنت. ✓ بيان إجراءات الخروج من المواقف غير اللائقة. ✓ بيان إجراءات الحد من فرص الوقوع كضحية للتنمر عبر الإنترنت. ✓ بيان الخطوات الفعالة للتعامل مع مختلف مواقف التنمر عبر الإنترنت ومعالجتها.	✓ الالتزام بتوجيهات وسياسات وإجراءات الأمان. ✓ بيان وممارسة إجراءات استخدام الإنترنت بطريقة منضبطة ومثمرة (كمحاولة موازنة وقت الاتصال مع عدم الاتصال). وصف إجراءات الخروج من أحد المواقع غير اللائقة. ✓ وصف إجراءات تقليل فرص الوقوع كضحية للتنمر عبر الإنترنت. ✓ وصف الخطوات الفعالة للتعامل مع أحد المواقف التي يتم فيها التعرض للتنمر

	التنمر وغيرها من السلوكيات أو المحتويات غير اللائقة.	✓ الفهم التام لمتطلبات الأمان والسلامة الحالية.	عبر الإنترنت وتطبيقها.
عرض السلوكيات الآمنة على الأصدقاء وأفراد الأسرة والمجتمع وتشجيعهم عليها.		✓ السلامة الشخصية النموذجية في مجموعة متنوعة من المواقف.	✓ السلامة الشخصية النموذجية في مجموعة متنوعة من المواقف. ✓ إظهار الالتزام بمواصلة الاطلاع على مستجدات قضايا الأمان والبرامج وممارسات الأمان الفعالة. ✓ عرض الممارسات والسلوكيات الآمنة على الأصدقاء وأفراد الأسرة والمجتمع وتشجيعهم عليها.

2- **الأمن السيبراني**

الأمان الرقمي: التدرب على الاستراتيجيات الآمنة التي تضمن الحماية الشخصية وتساعد على الدفاع عن أمان الشبكة.

	K-6	9-7	13-10
	الممارسات الآمنة	**الممارسات الآمنة**	**الممارسات الآمنة**
أ. التعرف على مخاطر الإنترنت واتخاذ قرارات مستنيرة وإجراءات مناسبة لحماية النفس حال استخدام تقنيات وأنظمة تقنية ووسائط رقمية وتقنية معلومات.	✓ فهم المخاطر التي تهدد الأمان على الإنترنت، والضرر المحتمل الناتج من السلوكيات الاحتيالية المتعلقة بالأنظمة التقنية والوسائط الرقمية وتقنية المعلومات بما فيها الإنترنت (كفيروسات البريد الإلكتروني والدعاية الرقمية وبرامج التجسس والإعلانات المتسللة والبرامج الخبيثة وسرقة الهوية وعمليات الاحتيال بالتصيد والبريد غير المرغوب فيه والهندسة الاجتماعية). ✓ فهم الممارسات الأساسية والفعالة للأمان والمرتبطة بالأنظمة التقنية والوسائط الرقمية وتقنية المعلومات بما في ذلك الإنترنت (كاستخدام كلمات مرور قوية وحماية كلمة المرور وهوية المستخدم وعدم الإفصاح عن المعلومات الشخصية	✓ فهم ومناقشة المخاطر التي تهدد الأمان على الإنترنت والضرر المحتمل الناتج من التطبيقات الاحتيالية ذات الصلة بالأنظمة التقنية والوسائط الرقمية وتقنية المعلومات بما في ذلك الإنترنت (كفيروسات البريد الإلكتروني والدعاية الرقمية وبرامج التجسس والإعلانات المتسللة والبرامج الخبيثة وسرقة الهوية وعمليات الاحتيال عن طريق التصيد ورسائل البريد غير المرغوب فيه والهندسة الاجتماعية). ✓ بيان ممارسات الأمان الفعالة -بما يتجاوز المستويات الأساسية- فيما يخص بالأنظمة التقنية والوسائط الرقمية وتقنية المعلومات بما في ذلك الإنترنت، والتدرب عليها. ✓ إدراك وفهم الهدف من تدابير المحافظة على الأمان المتعلقة بالأنظمة التقنية	✓ فهم ومناقشة المخاطر التي تهدد الأمان على الإنترنت والضرر المحتمل الناتج من التطبيقات الاحتيالية ذات الصلة بالتكنولوجيا والأنظمة التكنولوجية والوسائط الرقمية وتكنولوجيا المعلومات، بما في ذلك الإنترنت (كفيروسات البريد الإلكتروني والدعاية الرقمية وبرامج التجسس والإعلانات المتسللة والبرامج الخبيثة وسرقة الهوية وعمليات الاحتيال عن طريق التصيد والبريد غير المرغوب فيه والهندسة الاجتماعية). ✓ التدرب على ممارسات الأمان الفعالة وتحليل كل ما يستجد من خيارات، أعلى من المستوى المتوسط، متعلقة بالأنظمة التقنية والوسائط الرقمية وتقنية المعلومات بما في ذلك الإنترنت والتقييم النقدي للموارد الرقمية. ✓ إدراك وفهم الهدف من تدابير المحافظة

	المهمة وتقليل وتقييم إعلانات الشاشات المنبثقة). ✓ إدراك وفهم الهدف من تدابير الحفاظ على أمان الأنظمة التقنية والوسائط الرقمية وتقنية المعلومات. ✓ مناقشة استراتيجيات إدارة المشكلات اليومية المرتبطة بالأجهزة والبرامج.	والوسائط الرقمية وتقنية المعلومات. الفهم التام لمتطلبات الأمان الحالية.	
ب. اتخاذ قرارات مستنيرة حول أنسب وسائل الحماية والممارسات الآمنة في مختلف المواقف.		✓ الالتزام بتوجهات سياسات وإجراءات الأمان والسلامة. استخدام استراتيجيات إدارة المشكلات اليومية المتعلقة بالأجهزة والبرامج بفعالية. ✓ استخدام استراتيجيات فعالة للاتصالات اللاسلكية (كالاتصال بنقاط Wi-Fi النشطة القانونية فقط، أو إغلاق هذه الخاصية، أو إغلاق خاصية مشاركة الملفات أو تشفير البيانات/المعلومات المهمة، أو استخدام وتحديث برامج مكافحة الفيروسات، أو استخدام جدار حماية، أو تحديث نظام التشغيل).	✓ ✓
ج. الالتزام بمواصلة الاطلاع على مستجدات قضايا الأمان والبرامج		✓ الممارسات الآمنة النموذجية في مختلف المجتمعات الرقمية.	✓

وممارسات الأمان الفعالة.

د. عرض الممارسات والسلوكيات الآمنة على الأصدقاء وأفراد الأسرة والمجتمع وتشجيعهم عليها.	✓ عرض الممارسات والسلوكيات الآمنة على الأصدقاء وأفراد الأسرة والمجتمع وتشجيعهم عليها.

3- **أخلاقيات الإنترنت:**

القضايا القانونية والأخلاقية: يتعرف الطلاب ويتدربون على الاستخدام المسؤول واللائق للإنترنت أو التعاون مع الغير من خلال الشبكة وعند إبداع أنظمة تقنية ووسائط رقمية وتقنية معلومات. كما يبدون فهمًا للمعايير الأخلاقية والقانونية المعمول بها حاليًّا والحقوق والضوابط التي تحكم التقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات في سياق مجتمع اليوم.

ملحوظة: من الاستخدام غير اللائق –على سبيل المثال لا الحصر- عرض أي محتوى غير مهذب أو استخدام شبكة المدرسة لأغراض غير تعليمية أو استخدام شبكة العمل في أنشطة ليست ذات صلة بالعمل أو إرسال معلومات غير صحيحة أو غير دقيقة أو التنمر أو المشاركة في مجموعات معادية أو التحرش أو إرسال تعليقات خبيثة أو ممارسة القرصنة الإلكترونية أو التنزيل غير القانوني للمواد أو الأفلام أو الموسيقى الخاضعة لحقوق الطبع والنشر، ونسخ هذه المواد ونشرها وغير ذلك.

	K-6	9-7	12-10
أ. شرح السياسات المقبولة واتباعها (بالمدرسة والمنزل والمجتمع) وإدراك العواقب الشخصية والمجتمعية التي تنجم عن الاستخدام غير اللائق.	✓ شرح سياسات الاستخدام المقبولة واتباعها (في المدارس والمنازل والمنشآت الاجتماعية مثلا). ✓ مناقشة القضايا الأساسية ذات الصلة بالاستخدام المسؤول للتقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات، وشرح العواقب الشخصية التي تنتج من الاستخدام غير المسؤول*.	✓ الإقرار بسياسات الاستخدام المقبول واتباعها (كما في المدارس والمنازل والمنشآت الاجتماعية). ✓ التمسك بالاستخدام المسؤول للتقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات في مختلف المنشآت (كالمدارس والمنازل والمنشآت الاجتماعية)، وبيان وتحليل العواقب الشخصية والمجتمعية للاستخدام غير اللائق).	✓ الإقرار بسياسات الاستخدام المقبول واتباعها (كما في المدارس والمنازل والمنشآت الاجتماعية). ✓ التمسك بالاستخدام المسؤول للتقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات في مختلف المنشآت (كالمدارس والمنازل والمنشآت الاجتماعية)، وبيان وتحليل العواقب الشخصية والمجتمعية للاستخدام غير اللائق. ✓ تبني خيارات مستنيرة حول الاستخدام المقبول للتقنيات والوسائط الرقمية والأنظمة التقنية عند التعرض لمشكلات في الاستخدام.
ب. التمسك بالسلوكيات الأخلاقية والقانونية بين الأقران والأسرة والمجتمع وتشجيعهم عليها.			✓ بيان السلوكيات القانونية والأخلاقية حول الاستخدام المسؤول للتقنيات والأنظمة التقنية والوسائط الرقمية وتقنية المعلومات للأصدقاء وأفراد العائلة والمجتمع وتشجيعهم عليها.

ج. الالتزام بذكر مصادر المعلومات النصية والرقمية واتخاذ قرارات مستنيرة بشأن أفضل الطرق لتجنُّب السرقات الأدبية.	✓ شرح قواعد السلوك الأخلاقية واتباعها (كسياسة الاستخدام المقبول وكتيبات الطلاب ومدونة قواعد السلوك الطلابي ومواثيق الشرف). ✓ مناقشة التعريفات والمفاهيم والقضايا الأساسية المتعلقة بالسرقة الأدبية أو الغش الإلكتروني وبيان العواقب الشخصية والمجتمعية للسرقة الأدبية. ✓ إبراز الاستراتيجيات الملائمة لتجنُّب السرقات الأدبية (كالاقتباس وذكر المواضع والاعتراف بالمصادر وإعادة الصياغة). مناقشة أهمية احترام حقوق الغير فيما يخص عمله.	✓ الإقرار بقواعد السلوك الأخلاقية واتباعها (كسياسة الاستخدام المقبول وكتيبات الطلاب ومدونة قواعد السلوك الطلابي ومواثيق الشرف). مناقشة التعريفات والمفاهيم والقضايا الأساسية المتعلقة بالسرقات الأدبية أو الغش الإلكتروني وبيان العواقب الشخصية والمجتمعية للسرقات الأدبية. ✓ الالتزام بذكر مصادر المعلومات النصية والرقمية. تحديد أفضل استراتيجيات لتجنب السرقات الأدبية (كالاقتباس وذكر المواضع والاعتراف بالمصادر وإعادة الصياغة) والتدريب على استخدامها.	✓ الإقرار بقواعد السلوك الأخلاقية واتباعها (كسياسة الاستخدام المقبول وكتيبات الطلاب ومدونة قواعد السلوك الطلابي ومواثيق الشرف). مناقشة التعريفات والمفاهيم والقضايا الأساسية المتعلقة بالسرقة الأدبية أو الغش الإلكتروني وبيان العواقب الشخصية والمجتمعية للسرقة الأدبية. ✓ استعراض أنسب الاستراتيجيات لتجنب السرقات الأدبية (كالاقتباس وذكر المواضع والاعتراف بالمصادر وإعادة الصياغة). تحديد أكثر الطرق ملائمة لتجنُّب السرقات الأدبية وإنشاء أعمال أصلية، والالتزام بذكر مصادر المواد النصية والرقمية. ✓ ذكر السلوكيات الأخلاقية للأصدقاء وأفراد الأسرة والمجتمع وتشجيعهم عليها.
د. اتخاذ قرارات أخلاقية وقانونية عند مواجهة أي	✓ مناقشة التعريفات والمفاهيم والقضايا الأساسية المتعلقة بالملكية الفكرية	✓ مناقشة التعريفات والمفاهيم والقضايا الأساسية المتعلقة بالملكية الفكرية وقوانين	✓ مناقشة التعريفات والمفاهيم والقضايا الأساسية المتعلقة بالملكية الفكرية وقوانين

مشكلات في استخدام التقنيات والوسائط الرقمية والأنظمة التقنية.	وقوانين حقوق طبع ونشر الوسائط والمجالات الخاصة والعامة والاستخدام العادل ومشاركة الملفات. ✓ بيان العواقب الشخصية والمجتمعية لعدم احترام الحقوق والقوانين وحقوق الطبع والنشر والمجالات العامة والخاصة والاستخدام العادل ومشاركة الملفات. شرح سياسات الوصول إلى موارد المعلومات المعمول بها في المدارس والمنازل والأماكن الاجتماعية واتباعها.	حقوق طبع ونشر الوسائط والمجالات الخاصة والعامة والاستخدام العادل ومشاركة الملفات. ✓ بيان العواقب الشخصية والمجتمعية لعدم احترام الحقوق والقوانين وحقوق الطبع والنشر والمجالات العامة والخاصة والاستخدام الأمين ومشاركة الملفات. ✓ شرح سياسات الوصول إلى موارد المعلومات المعمول بها في المدارس والمنازل والمجتمع والالتزام بالقوانين المحلية وقوانين الولايات والقوانين الفيدرالية واتباعها. ✓ استعراض السلوكيات الاجتماعية والأخلاقية المناسبة عند استخدام التقنيات والوسائط الرقمية بما في ذلك التعرف على حقوق الملكية الفكرية والاستخدام الأمين للمواد الخاضعة لحقوق الطبع والنشر والمشاركة المشروعة للملفات أو تنزيل البرامج والموسيقى والفيديو. ✓ الاستفادة من الاستخدام الأخلاقي	حقوق طبع ونشر الوسائط والمجالات الخاصة والعامة والاستخدام الأمين ومشاركة الملفات. ✓ بيان العواقب الشخصية والمجتمعية لعدم احترام الحقوق والقوانين وحقوق الطبع والنشر والمجالات العامة والخاصة والاستخدام الأمين ومشاركة الملفات. ✓ بيان العواقب الشخصية والمجتمعية الناجمة عن الإخلال بحقوق الملكية الفكرية وقوانين حقوق طبع ونشر الوسائط والمجالات العامة والخاصة والاستخدام الأمين والمشاركة في الملفات. الإقرار بسياسات الوصول إلى موارد المعلومات المعمول بها في المدارس والمنازل والمجتمع والالتزام بالقوانين المحلية وقوانين الولايات والقوانين الفيدرالية واتباعها. ✓ التمييز بين الآثار القانونية للاستخدامات الشخصية والتعليمية والتجارية للأعمال الخاضعة للحماية.

		والقانوني للتقنيات والوسائط الرقمية والأنظمة التقنية وتقنية المعلومات عند التعرض لمشكلات في الاستخدام.	✓ استعراض السلوكيات الاجتماعية والأخلاقية التي ينبغي اتباعها عند استخدام التقنيات والوسائط الرقمية فيما يتعلق بالإقرار بحقوق الملكية الفكرية والاستخدام الأمين للمواد الخاضعة لحقوق الطبع والنشر، بما في ذلك المشاركة المشروعة للملفات أو تنزيل البرامج والموسيقى والفيديو. الاستفادة من الاستخدام القانوني والأخلاقي للتقنيات والوسائط الرقمية والأنظمة التقنية وتقنية المعلومات عند مواجهة مشكلات في الاستخدام. استعراض السلوكيات الأخلاقية والقانونية في هذا المجال مع الأصدقاء وأفراد الأسرة والمجتمع وتشجيعهم عليها.
هـ. بيان المسؤولية وآداب التعامل (مهارات الاتصال الرقمي اللائق) عند التواصل مع الغير رقميًا	✓ التعرف على الفروق الشخصية والالتزام بآداب التعامل في مختلف المواقف. ✓ التعرف على السلوكيات الاجتماعية والأخلاقية الإيجابية والسلبية عند استخدام التقنيات والوسائط الرقمية	✓ التعرف على الفروق الشخصية وممارسة آداب التعامل داخل المجتمعات الرقمية المتنوعة. ✓ التعرف على السلوكيات الاجتماعية والأخلاقية الإيجابية والسلبية عند استخدام التقنيات والوسائط الرقمية وتقنية	✓ التعرف على الفروق الشخصية وممارسة آداب التعامل داخل المجتمعات الرقمية المتنوعة. ✓ إدراك وتحليل السلوكيات الاجتماعية والأخلاقية الإيجابية والسلبية عند استخدام التقنيات والوسائط الرقمية وتقنية

	وتقنية المعلومات.	المعلومات.	المعلومات.
و. التعرف على الدلائل والآثار الشعورية والعواقب القانونية للتنمر عبر الإنترنت والحلول الفعالة للتصدي له.	✓ شرح ومناقشة دلائل التنمر عبر الإنترنت والحلول التي يمكن اتباعها للتصدي له. التعرف على أنسب وقت ومكان لاستخدام الأدوات والتقنيات والموارد الرقمية (كالوقت المناسب لاستخدام اللغة العامية والرموز التعبيرية والوقت المناسب لاستخدام الهاتف المحمول والرسائل النصية). ✓ تطبيق مهارات الاتصال اللائقة عند التواصل الرقمي.	✓ إظهار فهم شامل للدلائل والآثار الشعورية والعواقب القانونية للتنمر عبر الإنترنت والحلول الفعالة للتعامل معها. ✓ التعرف على أنسب وقت ومكان لاستخدام الأدوات والتقنيات والموارد الرقمية (كالوقت المناسب لاستخدام اللغة العامية والرموز التعبيرية والوقت المناسب لاستخدام الهاتف المحمول والرسائل النصية).	✓ إظهار فهم شامل للدلائل والآثار الشعورية والعواقب القانونية للتنمر عبر الإنترنت والحلول الفعالة للتعامل معها. ✓ تبني خيارات مستنيرة عند التعرض لمشكلات تخص التنمر عبر الإنترنت. ✓ التعرف على أنسب وقت ومكان لاستخدام الأدوات والتقنيات والموارد الرقمية (كالوقت المناسب لاستخدام اللغة العامية والرموز التعبيرية والوقت المناسب لاستخدام الهاتف المحمول والرسائل النصية). ✓ تطبيق مهارات الاتصال المناسبة عند التواصل الرقمي. التدرب على آداب التعامل الرقمي لتعزيز التعاون مع الغير، وتشجيع السلوكيات المراعية لآداب التعامل على الإنترنت بين الأصدقاء وأفراد الأسرة والمجتمع.
ج. التعرف على الوقت	✓ شرح أن المحتوى المنشور على	✓ شرح أن المحتوى المنشور على الإنترنت	✓ شرح أن المحتوى المرسل إلى الإنترنت أو

والمكان المناسبين لاستخدام الأدوات والتقنيات والموارد الرقمية.	الإنترنت أو المرسل عبر أي وسيلة رقمية أخرى (كالهواتف المحمولة والكاميرات) قد يطلع عليه عدد كبير من الناس، كما يمكن أرشفته بصورة دائمة.	أو المرسل عبر أي وسيلة رقمية أخرى (كالهواتف المحمولة والكاميرات) قد يطلع عليه عدد كبير من الناس، كما يمكن أرشفته بصورة دائمة.	المرسل عبر أي وسيلة رقمية أخرى (كالهواتف المحمولة والكاميرات) قد يطلع عليه عدد كبير من الناس كما يمكن الاحتفاظ به بصورة دائمة.
ح. شرح أهمية إدارة الهوية على الإنترنت ومراقبتها وتشجيع الغير على إدراك أهميتها.	✓ شرح أهمية إدارة الهوية على الإنترنت ومراقبتها. التعرف على الاستخدامات الإيجابية والسلبية للمواد المُرسلة بوسائل إلكترونية من منظور إدارة السمعة على الإنترنت	✓ شرح أهمية إدارة الهوية على الإنترنت ومراقبتها. التعرف على الاستخدامات الإيجابية والسلبية للمواد المُرسلة بوسائل إلكترونية من منظور إدارة السمعة على الإنترنت استعراض الاستراتيجيات المناسبة لحماية ومراقبة الهوية الشخصية ودعمها دعمًا إيجابيًا – إدارة ومراقبة السمعة على الإنترنت.	✓ شرح أهمية إدارة الهوية على الإنترنت ومراقبتها. ✓ التعرف على الاستخدامات الإيجابية والسلبية للمواد المُرسلة بوسائل إلكترونية من منظور إدارة السمعة على الإنترنت. ✓ استعرض أنسب استراتيجيات لحماية ومراقبة الهوية الشخصية أو دعمها دعمًا إيجابيًا. تحليل الوسائط والمواد الإلكترونية المُرسلة والتأمل بصفة شخصية في مدى ملائمة كل منها لإدارة السمعة على الإنترنت.

القسم 8: سياسات الأمن السيبراني

8-1 المبادئ التوجيهية لسياسة الكتابة

8-1-1 السياسات اللازمة لحماية الطلاب

1- **ما مدى الاختلاف بين "السياسات" و"الإجراءات"، وهل الفرق مهم؟**

السياسات هي مبادئ أو قواعد تهدف إلى صياغة القرارات والإجراءات، كما توفر إطار عمل لأداء المؤسسات، أما الإجراءات فهي الطرق التي تُنفذ بها المؤسسات السياسات، وتجيب السياسات عن أسئلة "ماذا" و"لماذا"، أما الإجراءات فتجيب على أسئلة "كيف" و"مَن" و"متَى"، ويُعبر عن السياسات بعبارات شاملة، بينما يُعبر عن الإجراءات بعبارات سلوكية أو تشغيلية محددة، ويكمن الهدف الأساسي من السياسات في تمكين المعلمين والموظفين والطلاب من فهم مسؤولياتهم القانونية والأخلاقية فيما يتعلق بأنشطة السلامة الإلكترونية عبر الإنترنت.

وتتمثل الأهداف الرئيسية من وضع سياسات الأمن السيبراني في:

- ✓ الحد من تعرض الطلاب للضرر أو الخطر.
- ✓ الحفاظ على سلامة الطلاب والموظفين.

تعد طريقة النظر إلى تصرفات المعلم الفعلية أو المتصورة أو الضمنية من منظور أخلاقي أو قانوني أمرًا هامًا من حيث احترام نزاهتهم المهنية مع ضمان سلامة الطلاب، ويجب أن تعكس السياسات والممارسات المهنية فهمًا للخصائص المعنية بالتقنية والمعلومات الرقمية.لوضع سياسة للتعامل مع الأجهزة الرقمية ضع في اعتبارك الأسئلة التالية عند صياغة سياسة المدرسة لاستلام للتقنية الرقمية واستبقائها وتخزينها:

سياسة الاستسلام:

- ✓ كيف يساهم استسلام جهاز في الخروج من المأزق؟
- ✓ هل المعلومات الرقمية مخزنة بالفعل على هذا الجهاز؟ هل يوجد نسخ في مكان آخر؟
- ✓ هل ينبغي الحصول على استشارة متخصصة قبل تقديم الطلب لاستسلام الجهاز؟ هل هذه الخبرة متاحة داخليا؟

سياسة الاحتفاظ:

- ✓ من صاحب الجهاز؟هل الجهاز مملوك للطالب أو المدرسة أو جهة خارجية؟
- ✓ هل ينبغي الاحتفاظ بالجهاز كدليل للمناقشة مع أولياء الأمور أو الإدارة العليا أو الشرطة مثلا؟

سياسة التخزين:

قبل التخزين هل كان الجهاز:

- ✓ مقفلا بـ PIN أو كلمة مرور أو غيرها من وسائل المصادقة؟
- ✓ معزولا عن أي اتصال خارجي بإيقافه أو تحويله إلى "وضع الطيران؟"

يجب أن يتكون السجل من:

- ✓ الحادث وسبب طلب استسلام الجهاز
- ✓ وقت ومكان استسلام الجهاز
- ✓ الإجراء المتخذ لتأمين الجهاز قبل التخزين
- ✓ العاملين والطلاب المشاركين في الحادث
- ✓ خطة متابعة العمل

من العوامل التي يجب على المدارس مراعاتها عند الاحتفاظ بجهاز ما إذا كان:

- ✓ مستخدمًا للحفاظ على صحة وسلامة الطالب
- ✓ مستخدمًا للتعلم
- ✓ متورطا في حادث، ولا تقل شدة هذا الحادث عن السلوك غير القانوني.

2- سياسة السلامة على الإنترنت

يجب أن تتبع هذه السياسة القانون الاتحادي الذي ينص على ما يلي:

- ✓ وصول الصغار للموضوعات غير اللائقة على الإنترنت
- ✓ سلامة وأمن الصغار عند استخدام البريد الإلكتروني وغرف الدردشة وغيرها من أشكال الاتصالات الإلكترونية المباشرة
- ✓ الوصول غير المصرح به، بما في ذلك ما يسمى "القرصنة"، وغيرها من الأنشطة غير القانونية على الإنترنت من قبل الصغار
- ✓ كشف واستخدام ونشر غير مصرح به لمعلومات شخصية حول الصغار
- ✓ التدابير التي تقيد وصول الصغار إلى المواد الضارة بهم

3- سياسات التنمر المدرسية

يجب أن تشتمل سياسات التنمر في المدارس على إجراءات الوقاية والاستجابة، وبالتالي يجب أن يكون المعلمون على دراية بما يلي:

- ✓ الإقرار بأن سلوك التنمر يمثل مخاطرة يجب إدارتها بشكل ملائم
- ✓ إدراك مخاطر التنمر الإلكتروني وخطورة انتشاره
- ✓ توثيق السياسات والإجراءات التي تحدد كيف تمنع المدرسة بشكل استباقي سلوك التنمر من خلال بناء المهارات الاجتماعية للطلاب وخلق بيئة مدرسية آمنة
- ✓ استقصاء آراء الطلاب بانتظام حول موضوع الأمان (بما في ذلك سلوك التنمر)، واستخدام المعلومات لصياغة طرق التحسين
- ✓ توفير التطوير المهني المستمر لتدريب العاملين على التعرف على التنمر والاستجابة لهذه النوعية من السلوكيات
- ✓ توفير التوجيه والاستشارات المناسبة للطلاب
- ✓ تنفيذ استراتيجيات لمنع وإدارة التنمر
- ✓ دمج إدارة التقنيات الرقمية في الإستراتيجيات
- ✓ مراقبة نجاح الإستراتيجيات التي تم تنفيذها

8-1-2 المصادر الرئيسية لوضع السياسات الأمنية في المدرسة

هناك العديد من الموارد المعترف بها لمساعدة واضعي السياسات على تنظيم عملهم، وتجنب العثرات وتوفير المبالغ الهائلة. ويجب أن يتحرك المعلمون في إطار عمل لهيكلة استراتيجيات الحماية، وذلك من خلال إجراء التعلم والتوجيه والحماية:

1- **لتعلم**: ينمي الطلاب قدراتهم وقيمهم على تأمين أنفسهم وتأمين الغير عبر الإنترنت، ويمثل هذا جزء من المفهوم الأوسع "للمواطنة الرقمية".

2- **لتوجيه**: البرامج والممارسات والموارد الموضوعة لدعم تعلم الطلاب وتنمية ثقافة التقنيات الرقمية الإيجابية في المدرسة وفي المجتمع ككل. فمثلا يتم دمج السلامة على الشبكة في المناهج الدراسية، وتنمية قدرات المعلمين والقيادات، وتقوية العلاقات مع الأسرة، وإشراك الطلاب في التخطيط والتسليم.

3- **الحماية:** الأساليب الفنية لتقييد أو مراقبة الوصول إلى الإنترنت والسياسات التي وضعتها المدرسة والتي تخلق بيئة تعليمية رقمية آمنة ومأمونة. على سبيل المثال خطة الاستجابة للحوادث وقنوات الإبلاغ والسياسات المدرسية والقيود التقنية أو مراقبة الوصول للإنترنت.

وضع سياسة للاستفادة من الخدمات عبر الإنترنت في التدريس والتعلم. يوصى بأن تنظر المدارس فيما يلي..

1- **ملكية الحساب:**

- ✓ التأكد من أن كل طالب أو والد لديه حساب خاص به.
- ✓ تثبيط محاولة البعض لمشاركة تفاصيل تسجيل الدخول إلى الحساب.
- ✓ التأكد من أن سن الطلاب فوق الحد الأدنى للسن المسموح به لأصحاب الحسابات.
- ✓ وضع حدود مناسبة لكيفية استخدام الحساب للأغراض الشخصية والمدرسية. تشجيع الطلاب على التفكير في حذو سلوكيات لائقة على الإنترنت وإدارة ملفاتهم الشخصية على الشبكة.

2- **ملكية المحتوى:**

- ✓ التأكد من فهم حقوق موفري الخدمات في المحتوى الذي تم تحميله. تقرير ما إذا كان السلوك مقبولًا في سياق الأنشطة المخطط لها.

3- **الخصوصية**

- ✓ تشجيع الطلاب على النظر في خصوصيتهم على الإنترنت، على سبيل المثال، تأكد من الطلاب:
  - أ- قد فهموا جيدا ماذا يشكل معلومات تعريف شخصية وماهية المعلومات المرئية وتوجه لمن.
  - ب- قد فهموا كيفية استخدام المعلومات.
  - ج- تكون لديهم فهم بمن لهم صلاحية الوصول إلى المعلومات الخاصة بهم الآن وفي المستقبل.

- ✓ طرح توجيهات حول أنسب مستوى لإعدادات الخصوصية. على سبيل المثال هل يتم تبادل المعلومات بين زملاء الدراسة ومع الأسر وهل ستكون هذه المعلومات متاحة على الإنترنت ليجدها أي شخص ويعرضها؟
- ✓ هل يتم إشراك أطراف ثالثة كالمعلنين في المعلومات الخاصة؟ تقرير ما إذا كان السلوك مقبولًا في سياق الأنشطة المخطط لها.
- ✓ ضمان الامتثال لسياسات موفر الخدمة المتعلقة بالخصوصية والثقة والأمان.

4- التوجيه

- ✓ وضع سياسات محددة بشأن:
  - أ. التواصل مع الأسر والمجتمع ككل والاستعانة برأيهم في الموضوع.
  - ب. العلاقات عبر الإنترنت بين العاملين والطلاب.
- ✓ كيفية استخدام الإنترنت في أنشطة الحماية والتفاعل مع الحوادث. مثلا ضع في اعتبارك:
  - أ. خلق تواجد لوسائل التواصل الاجتماعي بالمدرسة تشجع على مشاركة الطلاب وأولياء الأمور.
  - ب. كيفية استخدام الإنترنت بشكل إيجابي عند الاستجابة لحادث ما.

3-1-8 موضوعات حول تقارير الأحداث

يجب إدراك المعلمين لدورهم في تعزيز العلاقات الصحية مع الطلاب لتشجيع السلوكيات اللائقة. يجب أن يركز المعلمين على:

1- تعزيز السلوك الإيجابي للطالب
2- إيجاد وسائل للتدخل المبكر والمستمر
3- منع السلوكيات غير اللائقة
4- التعامل مع السلوكيات غير اللائقة بعقوبات مناسبة.

ما المطلوب من المعلم القيام به؟

إبلاغ الإدارة بالحوادث الخطيرة التي يتعرض لها الطلاب، والاستجابة لجميع السلوكيات غير اللائقة، والتمسك بالاحترام داخل المدرسة أو خلال الأنشطة المدرسية أو في المواقف التي يكون للنشاط فيها تأثير سلبي على المناخ المدرسي.

ما هي أنواع الحوادث التي يتعين على المعلم الإبلاغ عنها؟

أبلغ عن أي أي حوادث خطيرة يتعرض لها الطالب ترى من وجهة نظرك أن إدارة المدرسة لابد أن تنظر فيها إما بالتعليق أو الإبعاد.

تشمل سلوكيات نشاط الطالب عبر الإنترنت التالي:

- التنمر بما في ذلك التنمر على الإنترنت
- القيام بإرسال الرسائل الإباحية والمواد الإباحية والتطرف أو أي أنشطة إنترنت أخرى غير قانونية.

كيف ينبغي على المعلم الإبلاغ عن الحادثة؟

اهتم بسلامة الآخرين ومدى حالة الطوارئ في الموقف عند الإبلاغ عن الحادثة. يجب توثيق بلاغك كتابة في الوقت المناسب من خلال استخدام الإبلاغ عن حوادث المدارس الآمنة.

ما هو السلوك الطلابي الذي يستلزم ردًا؟

- يجب الرد على أي سلوك طلابي يمكنه التأثير سلبًا على مناخ المدرسة.
- بالنسبة للحوادث التي لن يتم فيها النظر في إيقاف أو طرد الطالب، لكنك تشعر أنه ليس من الأمان الرد على ذلك فمن المتوقع أن تخبر المسؤول في أسرع وقت ممكن.

4-1-8 استبقاء أجهزة الطالب الرقمية والتخلي عنها

تتعرض حادثة أمن المعلومات لأي حدث بأي شكل من الأشكال للخطر بسبب الفقد أو التدمير أو التغيير أو النسخ أو النقل أو السرقة أو الاستخدام أو الوصول إليها بشكل غير قانوني أو عن طريق أفراد غير مصرح لهم سواء عن طريق الخطأ أو عن عمد, ويوضح المخطط المذكور أدناه ملخصًا بالخطوات والعمليات المشروعة التي تتناول استبقاء أجهزة الطالب الرقمية والتخلي عنها, لاحظ الأعداد المذكورة أدناه هي كالتالي:

1- **عملية الكشف:** كجزء من عملية التحقيق في الحادثة قد يحتاج المعلم إلى معرفة ما إذا كان الطالب قد شارك النص أو الصور مع أي شخص آخر (في الفصل أو خارجه) أو قام بتخزينها على أي جهاز رقمي آخر بما في ذلك خوادم "السحابة", ستسترشد عملية اتخاذ القرارات الخاصة بالمعلم بشأن ما إذا كان سيتم طلب الكشف عن هذا العنصر بعوامل ذات صلة بالحالة. قد تشمل التالي:

   - ✓ طبيعة النص أو الصور
   - ✓ إذا ما قام الطالب بمشاركة الصور عن طريق إرسالها إلى طلاب آخرين
   - ✓ الموقف والتأثير النفسي على الطلاب المتضررين
   - ✓ عمر الطالب ونضجه
   - ✓ أي عوامل أخرى ذات صلة

يمكن أن يشير عرض العنصر المطلوب إلى وجود عناصر أخرى مثيرة للقلق على الهاتف, ويمكن للمعلم أن يطلب من الطالب إظهار هذه العناصر, كما قد يشكل المعلمون اعتقادًا مبررًا حول وجود أجهزة أخرى تحت تصرف الطلاب الآخرين؛ الأمر الذي قد يؤدي إلى مطالبة كل طالب على حدة بالكشف عن العناصر الموجودة على هواتفهم.

2- **عملية التخلي عن الأجهزة الرقمية:** بعد أن تتاح للمعلم الفرصة لعرض النص أو الصور التي يمكنه/يمكنها تحديد نطاقها وطبيعتها، وعليه يُتخذ الإجراء اللاحق المطلوب تنفيذه, وتتمثل أحد الخيارات في طلب التخلي عن التكنولوجيا الرقمية, إذ ينبغي إتخاذ مثل هذا الإجراء في الحالات التي توجد فيها مخاوف مبررة كأن تكون البيانات الموجودة على أحد الأجهزة الرقمية ضارة ويحتاج الجهاز إلى الاحتفاظ به لمزيد من التحقيقات أو لمنع حدوث أضرار, كما ينبغي على المعلمين تجنب استخدام التخلي عن الأجهزة الإلكترونية كعقوبة, وينبغي أيضًا ملاحظة عدم إمكانية فصل المعلومات الرقمية بشكل مستقل عن الجهاز الذي تم التخزين عليه؛ الأمر الذي سيؤدي إلى خلق مزيد من النسخ الخاصة بهذه المعلومات, وفي حالة تخزين المعلومات الرقمية على الإنترنت فليس من الممكن تقنيًا طلب التخلي عنها, وفي هذه الحالة, سيحتوي الجهاز المتخلى عنه في أحسن الأحوال على نسخة من المعلومات التي تم إفشاؤها.

3- **إزالة مشكلة المعلومات الرقمية:** يمكن أن تساعد الإجراءات الفورية في منع المحتوى الإشكالي من الانتشار كما يمكن استخدامه كنهج فعال في تقليل أي محنة أو ضرر قد يحدث, ولذا فالاستجابة السريعة هي العامل الرئيس في تحقيق نتائج إيجابية, ومع ذلك لا يمكن حذف المعلومات الرقمية إلا بدقة تامة إذا تم إزالة جميع النسخ ولا يمكن استعادتها أو الوصول إليها من مصدر آخر, سيستلزم طلب حذف المعلومات الرقمية فقط:

- ✓ فهم واضح لما يهدف هذا الإجراء لتحقيقه واحتمالية نجاحه
- ✓ معرفة أن هذا الإجراء قد يتسبب في انقطاع أو إضافة المدرسة إلى سلسلة من الأدلة
- ✓ تقييم إذا ما كنت تريد حذف المعلومات الرقمية المتضمنة بعض الأسئلة مثل:

أ. ما المشكلة التي تحاول حلها؟ هل سيحقق هذا الإجراء النتيجة المرجوة؟ ما هي مسارات العمل الأخرى التي يمكن أن تساعد في حل هذه المشكلة؟

ب. هل المعلومات الرقمية غير قانونية أو غير لائقة؟ هل ستكون هناك حاجة إلى طلب المعلومات لاحقًا كدليل, على سبيل المثال المناقشة مع أولياء الأمور أو الإدارة العليا أو الشرطة؟

ج. ما نوع المعلومات الرقمية المتسببة في المشكلة؟ هل هي صورة أو فيلم أو نص؟ من صاحب هذه المعلومات؟ من لديه حق الوصول إليها؟

د. هل يحتاج طرف آخر إلى تسهيل عملية حذف المعلومات, على سبيل المثال أحد مزودي خدمة مواقع التواصل الاجتماعي؟

✓ في حالة إذا ما كان الحذف هو الرد المناسب:

أ. هل الجهاز متصل بالإنترنت؟ هل تم بالفعل توصيل المعلومات؟ لو الأمر كذلك, كيف وأين؟

ب. أين تم تخزين المعلومات؟ هل تم ذلك على جهاز أم على محتوى موقع ويب؟ هل يلزم كلمة مرور للوصول إلى المعلومات؟

ج. كم عدد المواقع الأخرى التي قد تحتاج إلى حذفها؟ هل يمكن الوصول إليها؟

د. ما هي الضمانات المتاحة في حالة حذف العنصر وعدم استعادته لاحقًا؟

4- حذف المحتوى الإشكالي من وسائل التواصل الاجتماعي وخدمات الإنترنت الأخرى:

تمثل الحوادث بشكل متزايد تحديًا للمدارس التي تتضمن محتوى أو اتصالات تم تحميلها على وسائل التواصل الاجتماعي أو غيرها من خدمات الإنترنت, فقد يعد هذا غير لائق أو يحتمل أن يكون غير قانوني, ويمكن أن يكون لحذف هذا المحتوى تأثير فوري وإيجابي على هذه الأهداف, وفي معظم الحوادث, قد يعرف الهدف الجاني بالفعل مما يعني أن هناك احتمالًا كبيرًا بأن هوية الجاني يمكن اكتشافها, وفي حالة إذا ما تم معرفة هويته, فقد يُطلب من الشخص الذي نشرها أن يقوم بإزالة هذا المحتوى, كما يمكن للمدارس الاتصال بمزودي الخدمة مباشرة لطلب حذف المحتوى باستخدام وظائف الإبلاغ الخاصة بالخدمة, ومع ذلك, فقبل القيام بهذا ينبغي على المدارس الاتصال بخبراء المؤسسة الحكومية للحصول على مشورة بشأن أفضل مسار للعمل.

تمتلك المؤسسة الحكومية التالي:

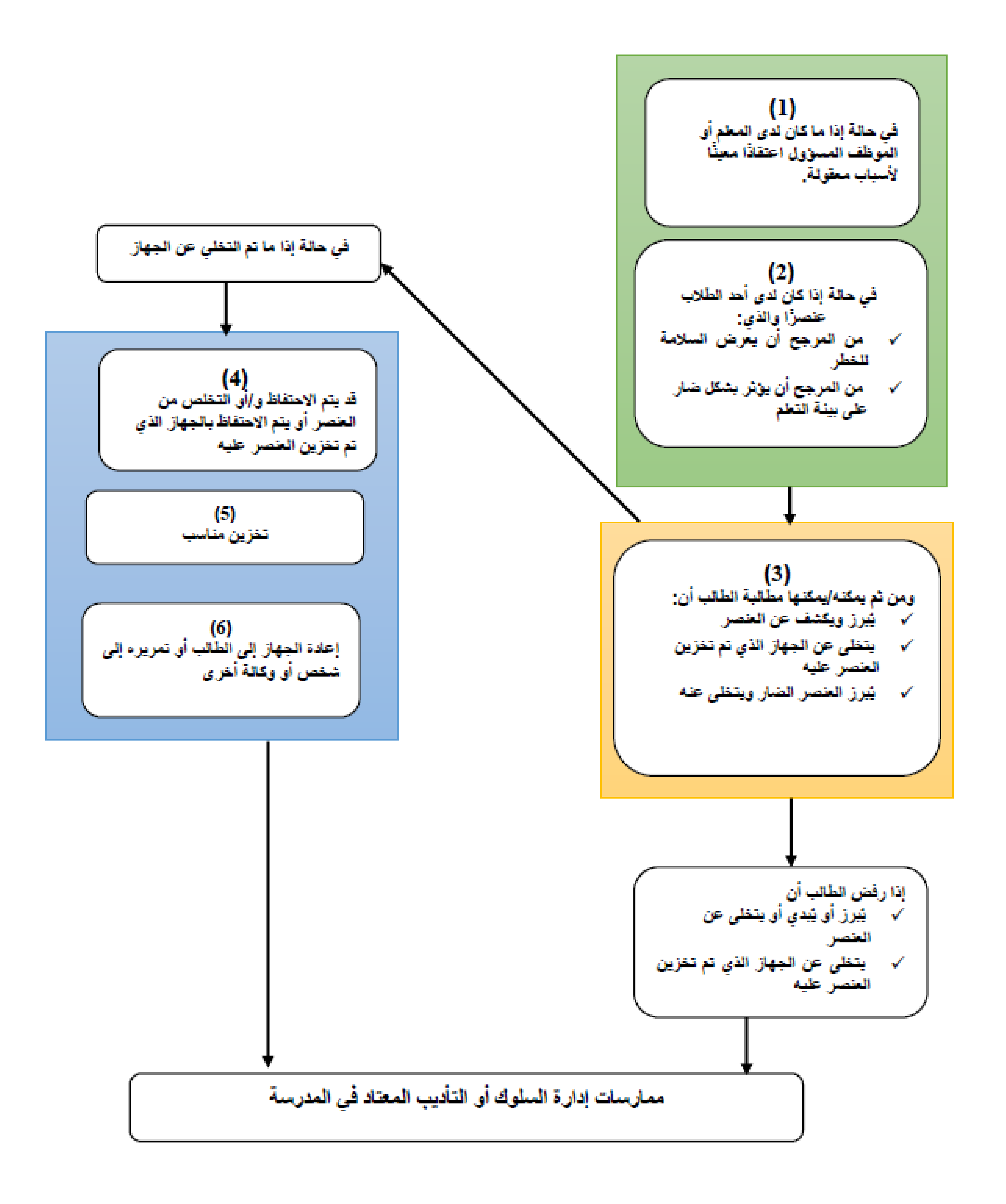
✓ خبراء في حل الحوادث التي تنطوي على محتوى غير لائق أو غير قانوني عبر الإنترنت والاتصالات

✓ متخصصين ذوي معرفة في خدمات وسائل التواصل الاجتماعي

✓ تأسيس علاقات عمل مع العديد من وسائل التواصل الاجتماعي الرائدة وغيرها من مقدمي الخدمات عبر الإنترنت.

كما يمكنهم تقديم المشورة للمدارس حول النجاح المحتمل لطلبات إزالة المحتوى، وحسب الاقتضاء يمكنهم العمل كوسيط لتسهيل هذه الطلبات, يمكن تحقيق ذلك عادةً في أطر زمنية أقصر بكثير مما يمكن للمدارس تحقيقه من خلال طلب مباشر إلى مزود الخدمة.

يتم تمثيل المعايير بالأرقام 1 و2 وعملية التخلي عن الأجهزة الرقمية برقم 3، وتمثل الأرقام 4 و5 و6 الاستبقاء/التخلص.



القسم 9: الأخلاقيات عبر الإنترنت

1-9 القضايا الأخلاقية الهامة المتعلقة بتعليم الأمن السيبراني



1-1-9 شروط ونظرية الأخلاق

1- شروط الأخلاقيات

- ✓ **قواعد الأخلاقيات:** تعمل على تحديد القيم الأساسية للمجال الطلابي وتوفُّر التوجيه لما ينبغي على المحترفين فعله عندما يواجهون التزامات أو مسؤوليات متضاربة في عملهم.
- ✓ **القيمة:** الصفات أو المبادئ التي يعتقد الأفراد أنها مرغوبة أو جديرة بالاهتمام، وهي تمنحهم قيمة لأنفسهم والآخرين والعالم الذي يعيشون فيه.
- ✓ **المبادئ الأخلاقية:** آراء الشعوب حول الصواب والخطأ؛ معتقداتهم وأفكارهم حول الكيفية التي ينبغي أن يتصرفوا بها.
- ✓ **الأخلاقيات:** هي دراسة للصواب والخطأ، والتي تنطوي على التفكير الناقد للأخلاق والقدرة على اتخاذ الخيارات بين القيم وفحص الأبعاد الأخلاقية للعلاقات.
- ✓ **الأخلاقيات المهنية:** هي الالتزامات الأخلاقية للمهنة والتي تنطوي على انعكاس أخلاقي يمتد ويعزز ممارسي الأخلاق الشخصية التي يجلبونها لعملهم، والتي تتعلق بالأفعال الصائبة والخطأ في مكان العمل، والتي تساعد الأفراد على حل المعضلات الأخلاقية التي يواجهونها في عملهم.
- ✓ **الرقابة** هي محاولة قمع أو تنظيم عملية وصول العامة إلى المواد التي تعتبر مسيئة أو ضارة.

2- بعض النظريات الأخلاقية

- ✓ **النسبية:** هي النظرية المقررة أنه لا يوجد قواعد أخلاقية عالمية للصواب والخطأ, وفقًا لهذه النظرية, يمكن أن يكون لدى الأفراد أو مجموعات مختلفة من الناس آراء متضادة كليًا لمشكلة أخلاقية وقد يكون كلاهما على صواب, فالنسبية الذاتية تؤكد أن كل شخص يقرر الصواب والخطأ لنفسه أو لنفسها, وقد أخذت هذه الفكرة من التعبير الشعبي "ما هو صحيح بالنسبة لك قد لا يكون مناسبًا لي".

- ✓ **النسبية الثقافية:** تقرر هذه النظرية الأخلاقية أن معنى الصواب والخطأ يقع على عاتق الإرشادات الأخلاقية الحقيقية للمجتمع, وتختلف هذه الإرشادات من مكان إلى آخر ومن وقت لآخر, على سبيل المثال, إذا قال أحد الطلاب الذكور كلمات غير لائقة لطالبة ما كأن يقترح عليها اقتراحًا مسيئًا أو يقوم بملامستها جسديًا بطريقة غير مناسبة ودون رضاها, فيُعد هذا التصرف غير مقبول ثقافيًا في منطقة مجلس التعاون الخليجي, **بينما قد يتم تجاهل مثل هذا التصرف في دول أخرى, ولكن نظرًا للطبيعة الدينية للثقافة المرتبطة بقوانين المجتمع فإن هذه السلوكيات غير مقبولة في بيئة مدرسية أو في أي مكان آخر في المنطقة.**
- ✓ **التصرف النفعي:** يعد هذا الإجراء جيدًا إذا تعدت فوائده أضراره ويعد سيئًا إذا تعدت أضراره فوائده, فهذه النظرية تنص على أن التصرف صواب (أو خطأ) بقدر ما يزيد (أو ينقص) من السعادة الكلية للأطراف المتضررة.
- ✓ **قواعد النفعية:** هذه هي النظرية التي تحتم علينا تبني هذه القواعد الأخلاقية التي إذا اتبعها كل شخص ستؤدي إلى زيادة أكبر في السعادة الكلية لكل الجماعات المتضررة, إذ تبحث قواعد النفعية في عواقب الإجراء.

2-1-9 قضايا أخلاقيات التعلم

1- أخلاقيات العلاقة مع الطلاب

تشكل هذه القواعد الأخلاقية أهمية قصوى بشأن حماية ورفاهية الطلاب.

- ✓ الاعتراف بمواطن الدعم والقوة الشخصية والمعرفة التقنية والتنوع والخبرة التي يجلبها الطلاب إلى بيئة التعلم.
- ✓ معرفة متطلبات المؤسسات الفردية للطلاب والتواصل بشكل مفتوح مع ممثلي تلك المؤسسة.
- ✓ تقديم النقد البناء المستمر وردود الفعل وكذلك التقييم العادل.
- ✓ تنفيذ الإستراتيجيات التي تشجع الطلاب وتمكنهم من تقديم مساهمات إيجابية لمكان العمل.
- ✓ الحفاظ على السرية فيما يتعلق بالطلاب.
- ✓ مد الطلاب بالفرص المهنية والمصادر حتى يتمكنوا من إظهار قدراتهم.
- ✓ إظهار قواعد السلوك هذه للطلاب من خلال الخبرة العملية حتى يلتزموا بهذه المعايير في مكان العمل.

- ✓ احترام كرامة وحقوق وآراء الآخرين ويتم احترام المعلمين لكرامة وحقوق وآراء الآخرين من خلال:
  - احترام الاختلافات الثقافية والعرقية والدينية
  - التقدير والاعتراف بالإسهامات التي قدمها الآخرون في تحقيق الأهداف المدرسية والإدارية

2- حماية الطلاب من الأضرار

يمكن للمعلمين حماية الطلاب من الأضرار عن طريق:

- ✓ إدراك أن للطلاب الحق في بيئة تعليمية آمنة ومأمونة
- ✓ قراءة واستيعاب والامتثال لمتطلبات الإبلاغ الإلزامية
- ✓ الإبلاغ عن أي شك مبرر بشأن الضرر الواقع على الطلاب
- ✓ تدعيم الطلاب المتضررين
- ✓ الامتناع عن السلوكيات التي قد تؤذي أو تضر بالطالب
- ✓ الامتناع عن السلوكيات التي قد تتسبب في أضرار نفسية للطالب
- ✓ الامتناع عن القيام بسلوكيات جنسية مع الطالب أو تلك التي من شأنها أن تزيد من مخاوف حدوث سلوك جنسي أو إمكانية حدوثه مع الطالب



3- **أخلاقيات استخدام الأجهزة الرقمية المدرسية**

أحد أهم الأمثلة على هذا النوع:

أ- احترام الملكية الفكرية

ب- الحفاظ على الخصوصية والأسرار الأخرى وعدم نشرها أو البحث عنها

ج- عدم إيذاء الآخرين

- ✓ عدم انتهاك الأجهزة الرقمية خاصة العامة منها مثل الأجهزة المدرسية
- ✓ التأكد من سلامة الأجهزة ومحتوياتها إما من الخدش أو الأحمال الثقيلة أو التسبب في إلحاق الضرر للجهاز.
- ✓ الحفاظ على الامتثال للقوانين المصممة لتنظيم استخدام الجهاز الرقمي، مثل الحفاظ على اسم المستخدم وكلمة المرور وعدم إعطائها للآخرين من الاستخدام غير المصرح به.
- ✓ عدم استخدام الكمبيوتر للإضرار بالآخرين
- ✓ عدم التدخل في عمل الطالب الآخر.
- ✓ عدم التجسس على ملفات الأجهزة الرقمية للطلاب الآخرين
- ✓ عدم استخدام الكمبيوتر في السرقة
- ✓ عدم نسخ أو استخدام برامج الملكية التي لم تدفع ثمنها
- ✓ عدم استخدام موارد أجهزة الطلاب الأخرى دون إذن أو تعويض مناسب

4- **أخلاقيات العمل مع مجموعات في الفصل:**

- ✓ أتفهم أنه ليس معنى أن الشئ قانوني أن يكون بالضرورة أخلاقي أو صواب.
- ✓ أتفهم أن الطلاب هم الذين يتضررون دائمًا عند استخدام الأجهزة بصورة غير أخلاقية, فالحقيقة بوجود أجهزة الكمبيوتر والبرمجيات أو وسائل الاتصالات بيني وبين هؤلاء المتضررين لا يغير على أية حال المسؤلية الأخلاقية تجاه أصدقائي البشر.
- ✓ أحترم حقوق المؤلفين، بما في ذلك مؤلفي وناشري البرمجيات وكذلك مؤلفي ومالكي المعلومات. أتفهم أنه ليس لمجرد سهولة نسخ البرامج والبيانات أنه بالضرورة أمر مشروع.
- ✓ لن اقتحم أو استخدم أجهزة الكمبيوتر الخاصة بالآخرين أو أقرأ أو استخدم معلوماتهم دون موافقتهم.
- ✓ لن أقوم بالكتابة أو الاقتناء أو التوزيع أو السماح بالتوزيع المتعمد للبرامج الضارة، مثل القنابل والديدان وفيروسات الكمبيوتر

3-1-9 قواعد الأخلاقيات والممارسات للمعلمين: الغرض والمجال والحالة

تهدف قواعد الأخلاقيات إلى تشجيع المعلمين على تبني نهج مستنير لتعاليمهم وعكسها على الممارسات الفعالة كمعلمين محترفين, حيث يجب أن يسعى المعلم كي يصير قدوة وأن يتصرف مع المجتمع بطريقة تحسن من مكانة المهنة.

1- الحفاظ على الثقة في مهنة التدريس

يجب على أعضاء مهنة التدريس القيام بما يلي:

- ✓ تأسيس علاقتهم مع الطلاب على الثقة والاحترام المتبادل
- ✓ مراعاة أن سلامة الطلاب ورفاهيتهم تقع ضمن مسئوليتهم
- ✓ احترام وحدة وتنوع المجتمع التعليمي الذين هم جزء منه
- ✓ العمل بطريقة تعاونية مع الزملاء وغيرهم من المهنيين
- ✓ تطوير العلاقات الجيدة مع الآباء وأولياء الأمور ومختصي الرعاية والحفاظ عليها
- ✓ التصرف بأمانة ونزاهة وعدالة
- ✓ الحساسية مع متطلبات السرية حيثما أمكن
- ✓ تولي مسئولية المحافظة على جودة ممارساتهم المهنية
- ✓ خلق خبرات تعليمية تعمل على إشراك الطلاب وتحفيزهم وحثهم على التحدي في بيئة شاملة من منظور تعليمي مدى الحياة

2- المحافظة على العلاقات المهنية مع الطلاب

- ✓ قم بالحفاظ على الحدود المهنية في المدرسة وخارجها وحاول تجنب الاتصال الجسدي غير الأخلاقي وعليك أيضًا تجنب الاتصال غير اللائق مع أي وسيلة من وسائل الإعلام كما يجب عليك تجنب العلاقات غير السليمة مع الطلاب, فأعضاء مهنة التدريس ملزمون بالواجب وهم مسؤولون في النهاية عن الحفاظ على مسافة مهنية
- ✓ الامتناع عن الاستفادة من العلاقات المهنية مع الطلاب لمصلحتهم الشخصية بما في ذلك إعطاء دروس خصوصية للطلاب من الفصل الذي يدرسون فيه أو الذين يخضعون لمسئوليتهم الإدارية مقابل الدفع سواء كانت نقدية أو عينية,
- ✓ إجراء التدخلات الرعوية مع الطلاب بصورة مهنية والتصرف بما يتماشى مع موقفهم الفريد من الثقة والمكانة كنماذج يحتذى بها.
- ✓ اتباع إدارة السلوك والسياسات والمبادئ التوجيهية للمدرسة الآمنة وفقًا لتوجيهات المدرسة والكليات والتعليم ذات الصلة.

- ✓ التصرف بشكل مناسب تجاه الطلاب الذين يمارسون الرعاية بلغتهم وإيماءاتهم ومواقفهم، مع ضمان عدم تصرفهم بطريقة محرجة أو مستهجنة وضمان أنهم لا يستخدمون لغة مسيئة أو أسماء عدوانية أو يقومون بتصريحات غير لائقة.
- ✓ التصرف بموقف وسلوك مهني في كل الأوقات

3- احترام تفرد وتنوع الطلاب

- ✓ عليك بإبداء الإحترام للتنوع الطلابي والمحافظة على العدل وتعزيز المساواة بغض النظر عن الجنس أو العرق أو الدين أو الميول الجنسية أو المظهر أو العمر أو اللغة أو الاحتياجات والقدرات الخاصة.
- ✓ الحفاظ على أن تكون المعرفة محدثة وفهم إجراءات حماية الطفل الحالية وتطبيقها والامتثال لها,
- ✓ الحفاظ على أن تكون المعرفة محدثة بالتوجيهات الصادرة على المستوى الوطني من قِبل مجلس مهنة التدريس ومدرستهم أو كليتهم أو السلطات التعليمية أو مكتب المفوض المعني بالطلاب بقدر ما يتعلق الأمر بسلوكهم الشخصي والمهني.
- ✓ المساهمة في خلق بيئة مدرسية عادلة وشاملة من خلال معالجة التمييز والقوالب النمطية والتنمر.

4- العمل بطريقة تعاونية مع الزملاء والآباء وأولياء الأمور وأخصائي الرعاية

- ✓ العمل بطريقة جماعية وتعاونية مع الزملاء وغيرهم من المهنيين الذين يعملون في فرق متعددة التخصصات معترف بها رسميًا من قبل السلطات التعليمية ؛
- ✓ احترام ودعم وتعاون مع الزملاء في الأمور المتعلقة بتعليم الطلاب وكذلك في الحفاظ على العلاقات مع الزملاء بأعلى معايير المجاملة المهنية؛
- ✓ تطوير العلاقات الجيدة بين المنزل والمدرسة والحفاظ عليها في ضوء احترام الدور الذي يلعبه الآباء وأولياء الأمور وأخصائي الرعاية في تعليم الطلاب
- ✓ الانخراط والعمل بشكل إيجابي مع أولياء الأمور -قدر الإمكان- بطريقة منفتحة ومحترمة
- ✓ تأكد من أن اتصالاتهم مع أولياء الأمور والطلاب والزملاء تمتثل للسياسات والإجراءات الصادرة على مستوى المدرسة أو الكلية، وكذلك السياسات والإجراءات التعليمية الصادرة على المستوى الوطني.

- ✓ إظهار الاحترام للتنوع عند التعامل مع الزملاء أو أولياء الأمور أو الأوصياء أو المهن بصفتهم شركاء في العملية التعليمية.
- ✓ بذل كل مجهود ممكن لتشجيع الآباء والأوصياء وأخصائي الرعاية على الإهتمام بنشاطهم في تعليم ورفاهية الطالب في رعايتهم.

5- التصرف بأمانة ونزاهة

- ✓ الامتثال للسياسات والإجراءات الصادرة في المدرسة أو الكلية أو مستوى التعليم الوطني فيما يتعلق باستخدام الممتلكات والمرافق والتمويلات وتكنولوجيا المعلومات والاتصالات في بيئتها التعليمية.
- ✓ إجراء التقييم والمهام المتعلقة بالفحص بنزاهة وبما يتوافق مع اللوائح والإجراءات الرسمية.
- ✓ تمثيل أنفسهم وتجاربهم ووضعهم المهني ومؤهلاتهم بأمانة.
- ✓ الكشف عن المعلومات السرية فقط ضمن المعايير المسموح بها في التشريعات
- ✓ مراعاة وضعهم كنموذج يحتذى به للطلاب.
- ✓ في كل من حياتهم الشخصية والمهنية يجب مراعاة سلوكهم وتصرفاتهم كونهم قد يكون لهم تأثير على المهنة التي يمثلونها.

4-1-9 ما الذي يتعين على المعلمين فعله في حالات معينة

المبدأ العام هو أن تركز أكثر على السلوك المتضمن في أحد الحوادث وبدرجة أقل على التكنولوجيا الرقمية. ليس من المتوقع أن تكون المدارس خبراء في الطب الشرعي الرقمي ويجب أن تستخدم جميع سبل التحقيق الأخرى المفتوحة أمامهم. على سبيل المثال نظرًا لأن هناك علاقة وثيقة بين السلوكيات في وضع عدم الاتصال وغير المتصل فهناك احتمال كبير أن يعرف الطالب الذي تعرض للمضايقة عبر الإنترنت هوية الجاني. ومن المحتمل أيضًا أن يكونوا غير مرتبطين في العالم الحقيقي وتكون المضايقات من نفس الشخص.

1- يمكن للمعلم أن يطلب من الطالب ما يلي:

- ✓ أن يقوم بحذف العنصر إذا كان ذلك مناسبًا
- ✓ أن يتخلى عن الجهاز الرقمي الذي تم تخزين العنصر عليه
- ✓ أن يحتفظ بالجهاز الرقمي المتخلى عنه لفترة معقولة وحينما يكون العنصر في حوزته يجب الاعتناء على نحو معقول بهذا العنصر، وإذا كان الجهاز سيُحتفظ به لمدة ليلة واحدة أو لفترة أطول فيجب تخزينه في مكان آمن.

يجب أن يتأكد المعلمون من وجود سجل للجهاز الرقمي وأن يقوموا بحفظه, ويتاح لهم يومان لإكمال هذا السجل, ويجب أن يعرض السجل ما يلي:

- ✓ تاريخ الحصول على الجهاز الرقمي
- ✓ اسم الطالب الذي تم أخذ العنصر منه

- ✓ اسم المعلم أو الفريق الذي قام بأخذ الجهاز

في نهاية فترة الاستبقاء، يجب على المعلمين إعادة الجهاز الرقمي إلى:

الطالب أو الشخص الذي ينتمي العنصر إليه أو نقله إلى أولياء الأمور/مقدمي الرعاية للطالب. في حالة الاشتباه في جريمة جنائية يجب تسليم الجهاز مباشرة إلى الشرطة, على سبيل المثال في حالة التورط في قضايا المخدرات والتهديد بالقتل أو الإيذاء البدني الجسيم أو المضايقة الجنائية.

2- لايمكن للمعلمين والفريق المسئول القيام بـ...

- ✓ مطالبة الطالب بالكشف عن العنصر الموجود على جهازه/جهازها أو أن يتخلوا عن جهازهم الرقمي دون وجود اعتقاد معقول أن عنصرًا ضارًا مُخزن على جهاز الطالب من المرجح أن يعرض الأمن النفسي للخطر أو يضر بالبيئة التعليمية.
- ✓ البحث في محتوى الجهاز الرقمي للطالب أو حساباته عبر الإنترنت
- ✓ مطالبة الطالب بإظهار كلمة المرور للوصول إلى الأجهزة الرقمية المخزن عليها العنصر
- ✓ مطالبة الطالب بتحميل و/أو الكشف عن العناصر الضارة المخزنة على جهاز رقمي آخر أو على وسيلة من وسائل التواصل الاجتماعي أو خدمة من خدمات الإنترنت الأخرى.
- ✓ استخدام القوة البدنية ضد الطالب

مطالبة طالبين أو أكثر بالكشف أو التخلي عن أجهزتهم الرقمية معًا دون إبداء اعتقاد معقول أن كل طالب لديه عنصر ضار من المرجح أن يعرض السلامة النفسية للخطر أو يؤثر سلبًا على البيئة التعليمية.

3- **التعرف على المتورطين في الحادث:** يمثل التعرف على المتورطين في الحادث أمرًا محوريًا من أجل إدارته الفعالة، كما أن استخدام التكنولوجيا الرقمية المعنية للقيام بذلك قد يكون أمرًا صعبًا، ومن ثم يجب على المدارس استخدام مجموعة من التحقيقات، بشكل عام هناك ثلاثة أدوار في الحوادث التي تنطوي على إساءة استخدام التكنولوجيا الرقمية

- ✓ مرتكبو الجرائم
- ✓ الشخص المستهدف
- ✓ المتفرجون

يمكن للعلاقات داخل هذه الفئات وفيما بينها أن تصبح معقدة بسرعة، فعلى سبيل المثال يمكن أن يكون الأشخاص المستهدفون والمتفرجون أيضًا من الجناة.

يوصى قيام المدارس بما يلي:

1- **تقديم سجل بكافة المعلومات المتاحة:** على الرغم من أن هوية الأشخاص الذين يقفون وراء صفحة ويب أو اتصال قد تكون مجهولة فمن المهم جمع كل المعلومات المتاحة قبل تغييرها أو إزالتها أو إخفاؤها، لذا يجب على المدارس النظر في طلب النصيحة من اختصاصي ما.

2- **البحث عن العلاقات بين السلوك على الإنترنت والسلوك غير المتصل:** الطلاب الذين تعرضوا للمضايقة عبر الإنترنت غالبًا ما يعرفون الجاني شخصيًا قبل وقوع الحادث، فمن المحتمل أنهم يتعرضون للمضايقة خارج شبكة الإنترنت أيضًا.

3- **الوعي بالدور المحوري للمتفرجين:** في علم النفس يشير "تأثير المتفرج" إلى الظاهرة التي يزداد فيها أعداد الأشخاص الحاضرين ويقل احتمال مساعدة الناس في حالة ضائقة، ففي معظم الحوادث عبر الإنترنت سيكون هناك متفرجين رقميين قد يكون دورهم إما سلبي أو إيجابي، وفيما هو متعلق بالطلاب ترتبط الثقافة التي تقود سلوك المتفرجين ارتباطًا وثيقًا بعلاقات الأقران، فهم و "تدمير" ثقافة المتفرجين هو نشاط للوقاية والرد.

9-1-5 كيف يجب على المعلمين مراقبة أنشطة الطلاب

يجب أن يعرف المعلمون أن البحث ليس حلاً عمليًا، ولا بد من المحافظة على سلامة المعلومات الرقمية المخزنة، ويمكن أن يؤدي إجراء البحث إلى تغيير المعلومات المخزنة على الجهاز، وعادة ما تقدم التقنيات الرقمية سجلاً للإجراءات التي تم تنفيذها، سيتم تسجيل أي محاولة للوصول إلى جهاز لإجراء عملية بحث؛ مما قد يعرض سلامة الطلاب والسلامة المهنية للمعلمين للخطر، ويمكن للطلاب الذي يدخلون على الأجهزة الرقمية للطلاب:

- ✓ توريط أنفسهم في تهم العبث بالجهاز أو المعلومات المخزنة عليه
- ✓ كسر سلسلة الأدلة التي يمكن استخدامها لمنع الضرر الذي يحدث للطالب أو في عمليات فرض القانون وإنفاذ القانون
- ✓ انتهاك حقوق الخصوصية للأشخاص الآخرين الذين لديهم معلومات مخزنة على جهاز، مثل الآباء والأمهات

المعرفة والأدوات المتخصصة مطلوبة لإجراء بحث مركّز بدلاً من "اختراق" المعلومات المخزنة على الجهاز، المعلومات التي يجرى البحث عنها قد تكون:

- ✓ جزء صغير من مجموعة واسعة من النصوص الورقية والصور والصوت والفيديو وغيرها من البيانات
- ✓ يتعذر الوصول إليها وذلك لأنها مُشفرة أو مصدقة
- ✓ ليست مخزنة على الجهاز لأنه إما قد تم حذفها أو أنها غير موجودة مطلقًا

9-2 المنظورات الأخلاقية المتعلقة بالاتصالات الشبكية

9-2-1 الأخلاقيات الواجب اتباعها عند إرسال الرسائل

الرسائل النصية تزيد إلى حد كبير من تعدد استخدام الهواتف المحمولة كمنصات لتبادل المعلومات، وبعض الاستخدامات المثيرة للإعجاب فيما يتعلق بالرسائل النصية للبلدان النامية.

1- لا تفتح أو تقبل أو تُحمل ملف يتعلق بالرسائل الفورية (رسالة فورية) من شخص لا تعرفه.

2- لا تفتح ملفًا من شخص لا تعرفه إلا إذا كنت تعرف محتويات الملف.

3- اتصل بالمرسل عن طريق البريد الإلكتروني أو الهاتف أو أي طريقة أخرى للتأكد من أن ما تم إرساله لا يحتوي على فيروسات.

4- إن الطلاب الأصغر سنا هم الأكثر تحمسًا للخوف من التعرض للعقاب بسبب السلوك السيئ، لكنهم يصبحون أكثر اهتمامًا بمكافآت السلوك الجيد مع تقدمهم في السن.

5- قد يشارك الطلاب العديد من الأفكار فيما يتعلق بالأمور الصحيحة والخاطئة مع الآخرين، لكنهم قد يتصرفون وفقًا لمبادىء يعتبرونها صحيحة حتى وإن كانت من منظور المجتمع أنها خاطئة، لذلك ينبغي أن يكون الطلاب على دراية بالقواعد والقوانين المتعلقة بإرسال الرسائل بطريقة فعالة.

9-2-2 أخلاقيات تفاعلات الإنترنت

1- تذكر أن الأشخاص الذين تتحدث معهم وتلعب معهم عبر الإنترنت هم أشخاص حقيقيون. حتى لو كنت لا تعرفهم، تخيل أنه أمامك مباشرة قبل أن تقول أو تكتب أي شيء.

2- تمهل في الرد، وإذا صدر أي شيء يزعجك أثناء الحديث معه، فتمهل قليلًا لتمتص مشاعر الغضب أو الخوف.

3- حاول التحدث إلى الشخص مباشرة بدلاً من الاتصال بالإنترنت، وتذكر أنه لا يمكن للآخرين معرفة ما تشعر به على الإنترنت أيضًا، لذلك من السهل أن تكون دراميًا.

4- تحدث إلى أصدقائك وعائلتك عما تشعر به، ويقول الطلاب الصغار باستمرار أن مجرد وجود شخص ما يستمع لهم هو واحد من أكثر الطرق فعالية للتعامل مع الصراع على الإنترنت.

5- لا تطلب الدعم-مرارًا وتكرارً- من مجموعتك حتى من أصدقائك ممن يوافقونك الراي، حيث يمكن أن يزيد ذلك الأمر من مشاعر الغضب.

6- راقب ما تشعر به، حيث يصعب اتخاذ القرارات الصحيحة حينما تنتابك حالة ضيق أو خوف أو ارتباك، وإذا تسارعت دقات قلبك أو انتابك شعورًا بالتوتر والضيق فاحرص على تسجيل الخروج من الإنترنت لبعض الوقت.

3-2-9 المبادئ الأخلاقية المتعلقة بالتنمر على الإنترنت

1- شجع الطلاب على أن يكونوا فعالين ومتسمين بالأخلاق عندما يتعرضون للتنمر، وقدم لهم نصيحة أفضل من مجرد "التصدي للهجمات"، فتختلف كل حالة من حالات التنمر عن نظيرتها، لذا نحتاج إلى تعليم الطلاب عند تعرضهم للتنمر أولاً "عدم إيذاء الغير" قبل القيام بأي أمر والتفكير في الكيفية التي قد تسوء بها الأمور.

2- علِّم الطلاب أن يفكروا قبل أن يتصرفوا، وامنحهم مجموعة من الأشياء للقيام بها عندما يتعرضون للتنمر، ويمكن أن تكون مواجهة الجاني علانيةً فعالة، ولكن في بعض الأوقات قد تجعل الجاني في موقف دفاعي خاصة إذا شعر بأنه هو المستهدف، وقد تكون المواجهة السرية فعالة للغاية وخاصة بين الأصدقاء، وفي الحالات التي يبدأ فيها السيناريو بالتحول إلى المضايقات فإن جهود الوساطة قد تكون قيمة للغاية.

3- بعد توثيق حالات التنمر والإبلاغ عنها أحد الردود المناسبة الأخرى، ولا سيما في بيئات الإنترنت التي تنطوي على إجراءات واضحة للإبلاغ عن التنمر، وتأكد من معرفة الطلاب بطرق الإبلاغ عن التنمر في كافة بيئات الإنترنت كشبكات التواصل الاجتماعي والألعاب الإلكترونية.

4- انقل بوضوح سلوك الطلاب المتوقع، وساعدهم على تطوير تفكير أخلاقي يركز بدرجة أكبر على القواعد والأعراف الاجتماعية بدلاً من الخوف من العقاب.

5- علِّم الطلاب إدراك متى يتحول المزاح إلى شيء جارح، وحثهم على التدخل عندما يتعرضون للتنمر.

6- يصبح -في حالة التدخل- التركيز على العاطفة ذي قيمة عند التعامل مع ضحايا التنمر، ولكن يتسم "المتنمرون الأذكياء" بأنهم جيدون في تبرير عدم شعورهم بالتعاطف، بل ويمكنهم حتى تحويل الأمر لمصلحتهم في التمادي في إزعاجهم للأشخاص.

7- شجع الطلاب على عدم إرسال أو الرد على شيء ما في حالة الغضب، بل "الابتعاد" عن الموقف والانتظار حتى تهدأ الأمور.

8- احرص على طمأنة الطلاب بأنهم غير مضطرين إلى مواجهة أي موقف بمفردهم، وتحدث إليهم حول المشكلات الإلكترونية في وقت مبكر قبل أن تسوء الأمور، واحرص على التواصل معهم كلما تقدموا في السن حتى يستطيعون طلب مساعدة شخص بالغ عندما يواجهون مشكلة.

9- يجب أن تتسم القواعد بالمرونة وتركز على حل المشكلات بدلاً من معاقبة مرتكبها.

10- يمثل توعية الطلاب بقواعد التنمر وقوانينه أكثر الطرق فاعلية لإحاطتهم علمًا بالأعراف الاجتماعية لعائلاتهم ومدارسهم ومجتمعهم.



9-2-4 طرق التعامل مع "إدمان الإنترنت"

يقضي بعض الأشخاص مقدار كبير من الوقت على الإنترنت غير أن علماء النفس يختلفون عما إذا كان من الممكن أن يتحول إلى إدمان على الإنترنت أم لا، وقد يكون استخدام الكمبيوتر الذي يدعم الإنترنت أمرًا ممتعًا، حيث إن هنالك عدد مذهل من الأمور يمكنك القيام بها على الإنترنت، وربما تعرف شخصًا يقضي كثيرًا من الوقت -ربما كثيرًا جدًا- في لعب ألعاب الكمبيوتر عبر الإنترنت، فهل هناك شيء كإدمان الإنترنت أو الألعاب الإلكترونية؟

1- يحتاج المعلمون وكذلك أولياء الأمور إلى التحدث مع طلابهم/أطفالهم لتوعيتهم بالمشكلة،

2- وعندما يقر الطلاب الشباب على وجود مشكلة (تلك هي الخطوة الأساسية) يجب عليك العمل معهم على وضع البرنامج يساعدهم على التغلب على هذه العادة.

3- لا يسمح المعلمين للطلاب بالدخول على أجهزة الكمبيوتر المتصلة بالإنترنت أثناء أوقات الراحة أو بين الدروس.

4- تحقق من برمجيات وأدوات الرقابة، وافرض قيودًا على استخدام الإنترنت.

5- في حالة عدم القدرة على السيطرة على سلوكيات الطلاب وأصبح الإنترنت يؤثر في جوانب أخرى من حياتهم فعليك طلب المشورة المهنية.

5-2-9 المبادئ الأخلاقية المتعلقة بمشاهدة الطلاب لمحتوى غير لائق واستخدامه

إن الصور غير اللائقة للأشخاص الذين لم تتجاوز أعمارهم 18 عامًا تُصنف على أنها "استغلال الأطفال إباحيًّا"، حيث إن اقتناءها أو توزيعها يُعد أمرًا غير قانونيًّا، وفي حين قد يُنظر إلى "الرسائل الجنسية" على أنها مقبولة أو ممتعة للطالب فعلينا أن ندرك جميعًا أن هذا قد يؤدي إلى عواقب فورية داخل البيئة المدرسية أو عواقب أكثر خطورة مع الشرطة.

1- تحدث إلى الطلاب بشأن الرسائل الجنسية وعواقبها - ولا تنتظر حدوث أي شيء.

2- قبل نشر أي منشور أو مشاركته عليك التفكير فيما ستشعر به في حالة نشر شخص ما صورة أو فيديو لك يشبه الذي بحوزتك!

3- أكد على أن القواعد والسياسات هي القواعد والأعراف الاجتماعية التي يتبعها كل فرد في مجتمعنا، سواء أكان ذلك المجتمع منزلًا أم مدرسةً.

4- استخدم الأدوات التكنولوجية المتاحة للمساعدة في الحد من تداعيات القرارات السيئة.

5- ضرورة تشجيع الطلاب على تبني عادة التفكير في شعور الشخص الذي يحتمل وجوده في الصورة أو الفيديو قبل نشره أو مشاركته.

6- يمكن أن تكون القواعد والقوانين ذات قيمة في مساعدة الصغار على اتخاذ القرارات السليمة بشأن المشاركة، ولا سيما مع الطلاب الشباب ولكنها تفرض قيوداً كبيرة.

7- ناقش المعضلات الأخلاقية المتعلقة بالرسائل الجنسية لتشجيع الطلاب على الارتقاء *بالأخلاق الشخصية التي ترشدهم* لاتخاذ قرارات جيدة.

8- كن قدوة حسنة حينما يتعلق الأمر بالقرارات الأخلاقية المتعلقة بالطلاب.

القسم 10: القوانين السيبرانية

10-1 التوعية والمبادئ التوجيهية بالجرائم الجنائية والالتزامات الأخلاقية

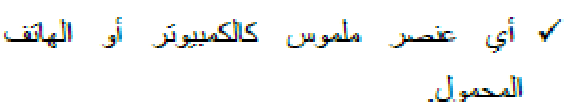
10-1-1 قضايا إدارة الحوادث

يجب على المعلمين أن يكونوا على اطلاع بالجوانب التالية للتشريعات التي تسري على إدارة الحوادث التي تتضمن استخدام الطلاب للأجهزة الرقمية بطريقة غير لائقة:

- ✓ وضع أسباب معقولة.
- ✓ الكشف والتخلي.
- ✓ الاحتفاظ بالأجهزة الرقمية والتخلص منها.
- ✓ الامتناع عن كشف عنصر ما أو تقديم الأجهزة الرقمية أو التخلي عنها.
- ✓ القيود المفروضة على صلاحيات المعلمين.
- ✓ عملية تقديم الشكاوى



الاعتقاد القائم على أسباب منطقية: قبل العمل بموجب التشريعات يجب أن يكون لدى المعلم أو أحد الموظفين المخولين أسباب منطقية للاعتقاد -أو التأكيد- بأن الطالب قد قام بإخفاء عنصر ما يُرجح تأثيره بصورة ضارة على بيئة التعلم أو يعرض سلامته للخطر، ووفقًا للتشريعات يمكن أن يكون العنصر المتعلق التكنولوجيا الرقمية:



- ✓ أي عنصر ملموس كالكمبيوتر أو الهاتف المحمول.



- ✓ أي معلومات رقمية مُخزنة على أي جهاز كمبيوتر وغيرها من الأجهزة الإلكترونية.

يتوقف الاعتقاد القائم على أسباب منطقية على ظروف العنصر وطبيعته، وقد يعتمد أيضًا عوامل أخرى أيضًا مثل سن الطالب ونضوجه، ويُعد الأمر متروك للحكم المهني للمعلمين لتحديد ما إذا كانت هناك أسباب معقولة لهم لاستخدام سلطاتهم القانونية لإدارة الحادث المطروح أم لا، فالهاتف الذكي كمثال لا يمثل أي خطورة على أي شخص أو يؤثر بصورة ضار على بيئة التعلم، ومع ذلك يمكن استخدامه لإرسال رسائل نصية غير مناسبة أو التقاط صور للطلاب في الفصل دون الحصول على موافقتهم، وفي تلك الحالة يمكن أن يكون معلم الفصل:

- ✓ لاحظ الطالب وهو يكتب الرسائل النصية أو يلتقط الصور.
- ✓ تلقى معلومات من مصادر موثوقة بأن الطالب قد أساء استعمال الجهاز الإلكتروني.
- ✓ تقدم طالب أخر شاهد النص الذي يتم إرساله أو الطلاب الذين تم التقاط صور لهم بشكوى للمعلم.

حينئذ يكون لدى المعلم اعتقاد قائم على أسباب معقولة بأن تصرف ذلك الطالب يمكن أن يؤثر تأثيرًا ضارًا على بيئة التعلم أو يعرض سلامة الطالب العاطفية أو الجسدية للخطر، وذلك بناءً على طبيعة النص أو الصور التي تم التقطها للطلاب.

2-1-10 ما يجب أن يعرفه المعلمون عن حماية الملكية الفكرية

1- **قانون براءات الاختراع:** ينص ذلك القانون على أن براءات الاختراع هي حقوق حصرية تُمنح للمخترعين للتشجيع على ابتكار اختراعات مفيدة ونشرها.

2- **قانون حقوق الطبع والنشر:** يشير إلى القوانين التي تجيز استخدام أعمال المؤلفين، مثل الكاتب والفنان وغير ذلك، ويشمل ذلك نسخ وتوزيع وتغيير الأعمال الأدبية وغيرها من الأعمال، ويحمل مؤلف أو كاتب أي عمل حقوق الطبع والنشر ما لم يرد ذلك في العقد، كما تندرج حقوق الطبع والنشر تحت مصطلح الملكية الفكرية إلى جانب الحقوق والاسم التجاري.

- ✓ يمكن تطبيق حقوق الطبع والنشر على أي عمل، ويشمل ذلك الفكرة الأصلية أو المؤلفات المستخدمة.
- ✓ تشمل حقوق الطبع والنشر أيضًا مجموعة واسعة من الابتكارات مثل أنواع الأعمال الفكرية والعلمية والفنية التي تشمل أيضًا القصائد وتأليف الأغاني والموسيقي ومقاطع الفيديو والرقصات والمنحوتات والبرمجيات، ويختلف الكثير منها بحسب السلطة المختصة أو القضائية.
- ✓ تُمنح حقوق الطبع والنشر إلى المؤلف وفقًا للقانون وبمجرد الانتهاء من عمله.
- ✓ ينبغي لك تسجيل العمل في مكتب حقوق الطبع والنشر من أجل حماية عملك وفكرتك.
- ✓ تجرم العديد من قوانين حقوق الطبع والنشر نسخ ملفات الترفيه.

الأعمال الفكرية التالية محمية بموجب قانون حقوق الطبع والنشر:

1- الكتب والكتيبات والمقالات وغيرها من المؤلفات.

2- برامج الحاسوب والتطبيقات وقواعد البيانات والأعمال المشابه المُحددة في القرار الذي أصدره وزير الاقتصاد.

3- المحاضرات والخطابات والخطب وغيرها من الأعمال ذات الطبيعة المماثلة.

4- المسرحيات والمسرحيات الموسيقية والتمثيليات الصامتة.

5- المسرحيات الموسيقية المصحوبة بحوارات والخالية من الحوارات.

6- أعمال الصوت والفيديو أو الأعمال السمعية والبصرية.

7- أعمال التصوير الفوتوغرافي.

يجب على المعلمين أن يكونوا على دراية بالقوانين التالية المتعلقة بالطلاب:

- ✓ لا يُسمح بنسخ البرامج المحمية بموجب حقوق الطبع والنشر دون إذن مُعد البرنامج.
- ✓ إبلاغهم بضرورة احترام قوانين حقوق الطبع والنشر وسياستها على الدوام.
- ✓ أخلاقيات حاسوب هي مجموعة من المبادئ الأخلاقية التي تتحكم في استخدام الحواسيب.
- ✓ تتمثل المشكلات الشائعة المتعلقة بأخلاقيات الحاسوب في مخالفات حقوق الطبع والنشر.
- ✓ يُعد نسخ المحتوي المحمي بحقوق الطبع والنشر دون موافقة المؤلف من أجل الحصول على معلومات شخصية تخص الآخرين من الأمثلة التي تنتهك المبادئ الأخلاقية.
- ✓ التوعية بقضايا حقوق الطبع والنشر أثناء استخدام المعلومات الإلكترونية.

3-1-10قوانين الخصوصية والسرية

احترام خصوصية الأفراد وسريتهم: مشاركة منشور عن شخص أخر دون الحصول على موافقته يمثل مخالفة، كما يُعد الإفصاح عن السرية مخالفة أيضًا كبرى.

- ✓ **الخصوصية والسرية**: يمكن أن ينشأ عن الإفصاح عن الأسرار المتعلقة بالحياة الخاصة لشخص معين دون موافقته مسؤولية قانونية، وبالمثل يمكن أن ينشأ عن الإفصاح عن المعلومات السرية مثل المعلومات التي تخص الطالب مسؤولية قانونية.
- ✓ **استخدام رموز المشاعر**: كن حريصًا عند استخدام أنواع محددة من رموز المشاعر أثناء التحدث عبر الإنترنت، على سبيل المثال إذا استخدم شخص الرمز التعبيري "الأصبع الأوسط" في محادثة ما، ومن ثم قام المستلم بتقديم شكوى بسبب ذلك الأمر الفعل؛ فقد يؤدي ذلك إلى إيداع الشخص في السجن أو تغريمه أو ترحيله.
- ✓ **العبارات التشهيرية**: يجرم قانون العقوبات نشر المعلومات التي تعرض شخصًا آخر للكراهية أو الازدراء العام أو تقديم اتهام زائف يفضح شخص آخر أو يشوه سمعته.
- ✓ **نشر الصور الفوتوغرافية**: يجب توخي الحذر عند نشر صور للآخرين عبر الإنترنت، بما في ذلك عبر مواقع التواصل الاجتماعي، حيث أن لأن قانون الجرائم السيبرانية (بوجه عام) يجرم استخدام أي وسيلة من وسائل تقنية المعلومات في انتهاك خصوصية شخص آخر، بما في ذلك التقاط صور للآخرين أو نشرها أو عرضها.
- ✓ **المحتويات المنافية للأخلاق والترابط الاجتماعي**: إن استخدام أي من وسائل تكنولوجيا المعلومات في الأنشطة غير المتوافقة مع الأخلاق العامة وحسن السلوك يُعد جريمة.

4-1-10 الأمور الواجب على المعلمين معرفتها بشأن مشاركة الملفات أو التنزيلات

لا يجوز بموجب قوانين حقوق الطبع والنشر تنزيل أو تحميل (مشاركة الملفات) أي مواد محمية بقانون الطبع النشر دون الحصول على تصريح من مالك حقوق الطبع والنشر، ويحظر قانون الطبع والنشر الأشخاص من تنزيل المواد أو تحميلها عبر منصات مشاركة الملفات مثل شبكات النظير للنظير، ويؤدي انتهاك هذا القانون إلى تعرض الأفراد إلى المسؤولية التضامنية أو المسؤولية عن المساهمة، فالمسؤولية عن المساهمة تتضمن معرفة شخص ما بانتهاك حقوق الطبع والنشر أو انتهاكها أو المساعدة في انتهاكها، أما المسؤولية التضامنية تحدث عندما لا يمنع أولياء الأمور صغارهم من انتهاك تلك الحقوق على الرغم من مقدرتهم على القيام بذلك، فعلى سبيل المثال قد يكون متعهد الأعمال مذنبًا عندما يفشل في استخدام سلطته لمنع طلابه من المشاركة في تبادل الملفات، وعندما يفكر المعلمون في مشاركة الملفات باستخدام شبكات النظير للنظير فهم بحاجة إلى فهم المشكلات الرئيسية التالية:

1- مخاطر الأمن والخصوصية:

- ✓ التسبب في تثبيت البرامج الضارة: عند تنزيل الملفات باستخدام تطبيقات النظير للنظير سيكون من الصعب التحقق من المصدر.
- ✓ تعريض الخصوصية للخطر: تبادل الملفات باستخدام تطبيقات النظير للنظير يمكن أن يوفر للأفراد إمكانية الدخول غير المرخص إلى المعلومات الشخصية والبيانات الحساسة (مشابهة لسجلاتك المالية والطبية) المخزنة على التطبيق أو على جهاز الكمبيوتر.
- ✓ الملاحقة القضائية: إذا قمت بتنزيل برامج مقرصنة أو مواد محمية بحقوق الطبع والنشر فقد تكون عرضة لإجراءات قانونية وغرامات باهظة حتى وإن لم تكن على دراية بذلك.

2- ما أنواع الأنشطة التي تمثل انتهاكات محتملة لقوانين حقوق النشر؟

أي من الأنشطة التالية إذا تمت دون إذن من مالك حقوق الطبع والنشر:

- ✓ نسخ ومشاركة الصور ومقاطع الموسيقى والأفلام والبرامج التلفزيونية أو غيرها من المواد المحمية بحقوق الطبع والنشر من خلال استخدام تقنية النظير للنظير.
- ✓ شراء المواد ثم عمل نسخ للآخرين.
- ✓ نشر المواد المحمية بحقوق الطبع والنشر أو سرقتها.
- ✓ تنزيل أو تحميل أي ملف لا يوجد لديك منه نسخه بالفعل.

3- أغلب القضايا القانونية الشائعة لمشاركة الملفات المتعلقة باستخدام تقنية النظير للنظير.

- ✓ الاهتمام بحقوق طبع ونشر الملفات وإما الحصول عليها أو عدم مشاركة الملفات.
- ✓ ينتهك مشاركو الملفات ومبرمجي برامج مشاركة الملفات قوانين حقوق الطبع والنشر الجنائية والمدنية.
- ✓ يجب وضع قوانين خاصة بحقوق الطبع والنشر.
- ✓ تحقق من أن المحتوى متاح قانونيًا.
- ✓ المحتوى مرخص ومتوفر مجانًا، فالكثير من ما هو متاح على شبكات النظير للنظير ليس كذلك.
- ✓ زيارة المواقع القانونية لمشاركة أو تنزيل الملفات القانونية؛ لتحميل ملفات ذات جودة أفضل.

5-1-10 المخاطر القانونية لوسائل التواصل الاجتماعي

قواعد يجب مراعتها:

- ✓ لا تنشر صور أو مقاطع فيديو لأشخاص آخرين دون الحصول على موافقتهم: لا تنشر بدون استئذان سواء أكنت صديقًا أم مصورًا، فقد تكون عملية النشر هذه انتهاكًا للخصوصية أو حقوق الطبع والنشر.
- ✓ لا تكون مصدرًا للتهديدات: المشاركات أو التعليقات المسيئة أو التي تهدد الآخرين يمكن أن تكون سببًا للمسائلة القانونية.
- ✓ لا تقم بالإشارة إلى أي شخص بدون الحصول على موافقته: يُعد الإشارة إلى أي شخص غالبًا بدون إذن انتهاكًا لقوانين التشهير والخصوصية؛ مما يترتب عليه غرامات كبيرة ويمكن أن تصل إلى السجن.
- ✓ لا تتنمر أو تتحرش: يجب على المستخدمين عدم نشر محتوى يتضمن كلامًا يحض على الكراهية أو يحرض على العنف أو يمثل تهديدًا أو يحتوي على مشاهد عنيفة أو غير مبررة.

يجب على المعلمين القيام بما يلي:

- ✓ مساعدة الطلاب على ضبط إعدادات الخصوصية الخاصة بهم بحيث تكون معلوماتهم محمية قدر الإمكان.
- ✓ مساعدة الطلاب على فهم سبب أهمية الحفاظ على خصوصية المعلومات الشخصية وقصرها على الأشخاص الذين يعرفونهم ويثقون بهم.
- ✓ تابع أصدقائهم وحاول معرفة مع من يتحدثون.
- ✓ تحدث إلى الطالب بشأن الرسائل الذي يتلقاها من أشخاص لا يعرفهم - أو الرسائل التي تكون سببًا في الشعور بعدم الارتياح أو الإحباط، ولتعلمهم أنه من المفيد أن يطلعوك على مثل هذه الرسائل وأن ذلك لن يُغضبك وأنك ستقدم لهم المساعدة.
- ✓ يجب عليك أيضًا وضع قواعد بشأن نشر الصور - سواء كان ذلك مسموحًا له القيام بذلك أم لا، تحقق من خلال شبكة الإنترنت على الرابط www.parentsprotect.co.uk؛ للحصول على موارد لمساعدتك في الحصول على رسائل أمان مهمة.
- ✓ كن حريصًا بشأن المعلومات التي تنشرها على شبكة الإنترنت، وعند نشر صورة أو مقطع فيديو تعرف على تفاصيل الحساب والوقت الذي سيبقى عليه من سيكون قادرًا على الاتصال به ورؤيته، فقد يسيئ مرتبكي جرائم الإنترنت استخدام ماقمت بنشره من صور.
- ✓ تذكر عدم وضع أي شيء شخصي على الإنترنت، مثل المعلومات الحساسة التي تخص عائلتك والعناوين والصور الشخصية التي من الممكن إساءة استخدامها.
- ✓ توفر معظم مواقع الويب والخدمات خيارات لإعدادات الخصوصية، واستخدم تلك الإعدادات لمنع مرتكبي الجرائم من مشاهدة المعلومات.
- ✓ يمكنك أيضًا ضبط إعدادات الخصوصية وفقًا لمن تسمح له برؤية معلوماتك.

تدريب عملي

السيناريو الأول: الصور الحميمية التي التقطت من خلال الهاتف الذكي

كان الطلاب "أ" و "ب" في علاقة انتهت بأمر مفزع، وقدمت الطالبة "أ" شكوى للعميد من أن الطالب "ب" لديه بعض الصور الحميمية التي تخصها على هاتفه الذكي وهددها بإرسالها إلى الأشخاص الأخرين، وكانت الطالبة "أ" مضطربة وطلبت من العميد مصادرة هاتف الطالب "ب" لحذف الصور.

1- **هل تُعد التصرفات غير القانونية تورطًا؟** قد يكون الفعل غير القانوني قد أُرتكب بالفعل، بناء على السياق المحيط، على سبيل المثال، الصور التي قام:

- الشخص "ب" بالتقاطها للشخص "أ" بدون معرفته أو الحصول على موافقة منه؟
- استخدم الصور لتخويف الطالب "أ" أو تهديده أو مضايقته؟

2- ينبغي أن يكون المعلم على دراية بالمشكلات التالية:

- ✓ إذا كانت الصور المنشورة من قِبل الطالب"ب" تمثل تهديدًا فإن ذلك يُعد انتهاكًا للقانون المدني (على سبيل المثال، فقد يمتلك الطالب"أ" حقوق الطبع والنشر للصور أو اقتحم خصوصيته من خلال هذا الإجراء).
- ✓ جريمة جنائية (على سبيل المثال إذا كان الطالب"أ" طفلًا).
- ✓ قد يكون هناك أيضًا تصرفات أخرى تثير المشاكل عبر الإنترنت أو خارج شبكة الإنترنت مثل التهديد أو الإيذاء البدني وفقًا للسياق.
- ✓ بغض النظر عما إذا كان السلوك غير القانوني يمثل تورطًا، فإن التصرف الذي ارتكبه الطالب "ب" غير مناسب وكان له تأثير مباشر على السلامة العاطفية للطالب وربما على بيئة التعلم الأوسع نطاقًا.
- ✓ يُعد دور المدرسة الرئيسي منع نشر الصور على شبكة الإنترنت لأنه إذا تم نشر تلك الصور فإن ذلك سيؤثر بالسلب على الطالب"أ" في المستقبل.

3- **هل مصادرة الجهاز إجراء يجب اتخاذه؟** يعتبر مصادرة الجهاز والاحتفاظ به من الإجراءات المناسبة لهذا السيناريو، ويرجع السبب الرئيسي في ذلك إلى وجود سبب وجيه للاعتقاد بأن الهاتف يوفر قناة لنشر الصور، فربما نُسخت الصور بالفعل إلى جهاز آخر أو حُملت على الإنترنت وربما إلى موقع تخزين الملفات على الويب.

4- **هل حذف الصور إجراء مناسب يجب اتخاذه؟** فيما يلي بعض الاستفسارات الأساسية التي تود المدرسة إخطارها لترى ما إذا كان طلب حذف الصور أمر مناسبًا أم لا:

- ✓ هل حذف الصور يؤدي إلى حل المشكلة وتقليل الضرر؟
- ✓ هل حذف الصور من الهاتف سيعمل على منع نشرها في المستقبل؟ (الإجابات المحتملة لهذه الأسئلة هي "لا" و "ربما".)

ملاحظة: *سيكون للحل الفعال تركيز قوي على سلوك الطالب "ب". على سبيل المثال، هل الطالب "ب"يكون على دراية بأن "الثقة في علاقة" هو مبدأ معترف به في القانون المدني والجنائي، ويجب معالجة هذه الصور الحميمية بصورة لائقة أثناء فترة العلاقة وبعد انتهاءها.*

5- **هل ذلك يُعد سلوكا غير لائق أو غير قانوني؟ عوامل يجب مراعاتها:**

- ✓ هل السن عامل مهم في هذا الحادث؟
- ✓ هل تم التقاط الصور سرًا ودون علم الشخص أو موافقته؟ (لاحظ أن الصور التي تلتقط بموافقة هي صور قانونية غير مدانة قانونيا).
- ✓ هل عنصر الإكراه متوفر؟ على سبيل المثال تم تم ممارسة الابتزاز بمزيد من الصور، أو صور الأصدقاء أو المال؟
- ✓ هل يتوفر عنصر من عناصر التهديد أو التخويف أو المضايقة بإلحاق أذى جسدي للشخص أو الممتلكات (على النحو المحدد في القانون)؟
- ✓ هل الصورة التي التقطها الطالب"أ" صور أصلية؟ وإذا كان الأمر كذلك فإن الطالب "أ" يملك حقوق الطبع والنشر، ولابد من استئذان صاحب الصورة الأصلي.

التعليقات:

- ✓ يُعد الهاتف والصور الملتقطة أمر مهم، لكن ينبغي أن يكون التركيز الأساسي على سلوك الطلاب.
- ✓ التهديد بنشر الصور تهديد صريح، لكن هل هو حادثة منعزلة؟ ما هو السياق الأعرض لهذا الحادث؟ هل استمرت المشكلات بين الطلاب لفترة، وكيف ظهرت تلك المشكلات؟ هل تم الإلمام بكافة جوانب المشكلة؟
- ✓ تعرف الطالب "أ" على الطالب "أ"، مما يعني أن إخفاء الهوية عبر الإنترنت لا يمثل مشكلة، ويمكن ترتيب مقابلة للطالبين بسهولة، ويتم الاتصال بوالديهم أو مقدمي الرعاية لهم إذا لزم الأمر.
- ✓ على الرغم من أنه قد تم التعرف على الطالب "ب" بسهولة، إلا أنه من المحتمل وجود "متفرجين" على هذا الحادث، هل من المفيد معرفة أماكنهم؟ إذا كانت الإجابة بنعم، فكيف ذلك؟

- ✓ هل حذف الصور رد مناسب لحل تلك المشكلة؟ فمثلا قد لا يحقق حذف الصور من الهاتف المحمول الهدف المنشود الذي نود الوصول إليه، ويتطلب حذف جميع النسخ معرفة جميع الأماكن التي تم تخزين الصور فيها والوصول إليها.
- ✓ فإذا تجاوزت عمليات النشر حدود المدرسة ونُشرت الصور على الإنترنت، فيمكن تقديم طلب إلى المستضيف لإزالتها، وارجع إلى NetSafe لمعرفة المزيد حول كيفية الخروج من تلك المشكلة.

السيناريو 2: الصور الإباحية على جهاز من الأجهزة الذكية للمدرسة

دعا الطالب"أ" مجموعة من الأصدقاء لمشاهدة موقع على الويب به صورًا إباحية ومشاهد عنف مستخدمًا الجهاز الذكي الخاص بالمدرسة (IPAD)، وقد انزعج طالب من الطلاب إثر مشاهدته ذلك المحتوى، وعلى الفور أبلغ أمين المكتبة بمصادرة الجهاز وفحصه.

الاستجابة للحادث: يطلب المعلم من الطالب تسليم الجهاز، ويقوم بفحصه حيث أن الجهاز ملك للمدرسة، وقد ترغب إدارة المدرسة في النظر في تلك المشكلات، وقد تطرح الأسئلة التالية:

- ✓ كيف تم الوصول إلى تلك الصور؟ من الإجابة على هذا السؤال ستتعرف الإدارة على ما إذا كانت هناك حاجة إلى التركيز على الجهاز الذكي فقط، أو أن تلك الصور موجودة على أجهزة أخرى أو خوادمها.
- ✓ هل تم الوصول إلى تلك الصور من خلال:
  - أ. تحميلها على جهاز زكي محليا. كاستخدام وحدة تخزين خارجية USB؟
  - ب. شبكة المدرسية؟
  - ج. الاتصال بالإنترنت الخاص بالطالب (ولكن عبر جهاز محمول مربوط بالإنترنت) أو اتصال طرف آخر (كشبكة Wi-Fi مجتمعية)؟
- ✓ فإن تم الوصول إلى تلك الصور عن طريق شبكة المدرسة فهل تم تجاوز أي نظام تأمين وحجب محتوى باستخدام شبكة خاصة افتراضية ((VPN؟ حساب شبكة من الذي تم استخدامه؟
- ✓ ما نوع الصور التي تم مشاهدتها؟ هل هي غير لائقة (أي محظورة) أو غير قانونية (أي مواد ممنوعة)؟
- ✓ هل تم عرض الصور كمحتوى غير قانوني؟ فإن كان الأمر كذلك فيجب تأمين الكمبيوتر المحمول إلكترونيًا وماديًا وإبلاغ إدارة الشؤون الداخلية عن الحادث.

- ✓ إذا كانت الصور غير لائقة فهل يكون ذلك دليلًا على إجراء تأديبي داخل المدرسة؟ فإن كان الأمر كذلك فيجب تأمين الجهاز الذكي إلكترونيًا وماديًا، واختبار الجهاز من قبل أخصائي أدلة جنائية رقمية نيابة عن مجلس إدارة المدرسة.
- ✓ هل يتم مراجعة إستراتيجيات الحماية في المدرسة بعد هذا الحادث؟ على سبيل المثال هل سياسات المدرسة المتعلقة بالاستخدام المناسب للتقنيات الرقمية محددة ومفهومة بوضوح لدي الطلاب؟ ما هو الدعم المقدم من الجهات الراعية للطلاب ممن يشاهدون المحتوى؟

السيناريو 3: تسجيل حادث في الفصل المدرسي

تولى أحد المعلمين أحد الفصول المشاغبة يوم الاثنين، وكانت هناك مشادة بينه وبين بعض الطلاب، وشمل ذلك اقتحام أحد الطلاب للفصل، واكتشف المعلم أن طالبًا قام بتسجيل هذا الحادث على هاتفه الذكي، وينوي تحميل الفيديو على الويب كنوع من المزاح، ويريد المعلم مصادرة الهاتف وحذف المحتوى؛ لأنه يرى أن ذلك سيكون أمرًا مهينًا واختراقًا للخصوصية لجميع المشاركين فيه.

الاستجابة للحادث:

هل حدث انتهاك للخصوصية؟

يخضع كل الطلاب للخصوصية (القانون)، ويتم تطبيق هذا القانون على "أي شخص أو مجموعة، سواء مجمعين أو منفردين"، من الناحية القانونية ينبغي النظر في الحوادث التي تنطوي على معلومات رقمية مخزنة على الهاتف الذكي أو أي جهاز محمول آخر على أساس كل حالة على حدة. وتوجد مجموعة من العوامل يجب أخذها بالحسبان في هذا الصدد، كمبادئ الخصوصية المطبقة وأي استثناءات للمبادئ القانونية نفسها، ويُنصح بالرجوع إلى سياسة خصوصية مجلس الأمناء فيما يتعلق بالقانون وطلب المشورة المتخصصة إذا لزم الأمر، وينبغي الاستحكام بسياسة خصوصية مجلس الأمناء في العمليات التي تتبعها المدرسة.

ما هي الخيارات الأخرى المتاحة للمدرسة؟

ينطوي الإجراء التهديدي والمتمثل في نشر الفيديو عبر الإنترنت أو مشاركة التسجيل بطريقة أخرى على ما يلي:

- ✓ التأثير بصورة ضارة على بيئة التعلم، أي تعطيل بيئة المدرسة بإثارة الشائعات والغمز وتدبير المكائد
- ✓ تعريض سلامة المعلم للخطر، أي إلحاق ضرر به من خلال التهديد المباشر للسلامة العاطفية للشخص.

ذلك الأمر يعطي للمدرسة حق التصرف في هذه الحالة، ويتم تطبيق النصيحة بالحذف الواردة في هذا الدليل في هذه الحالة.